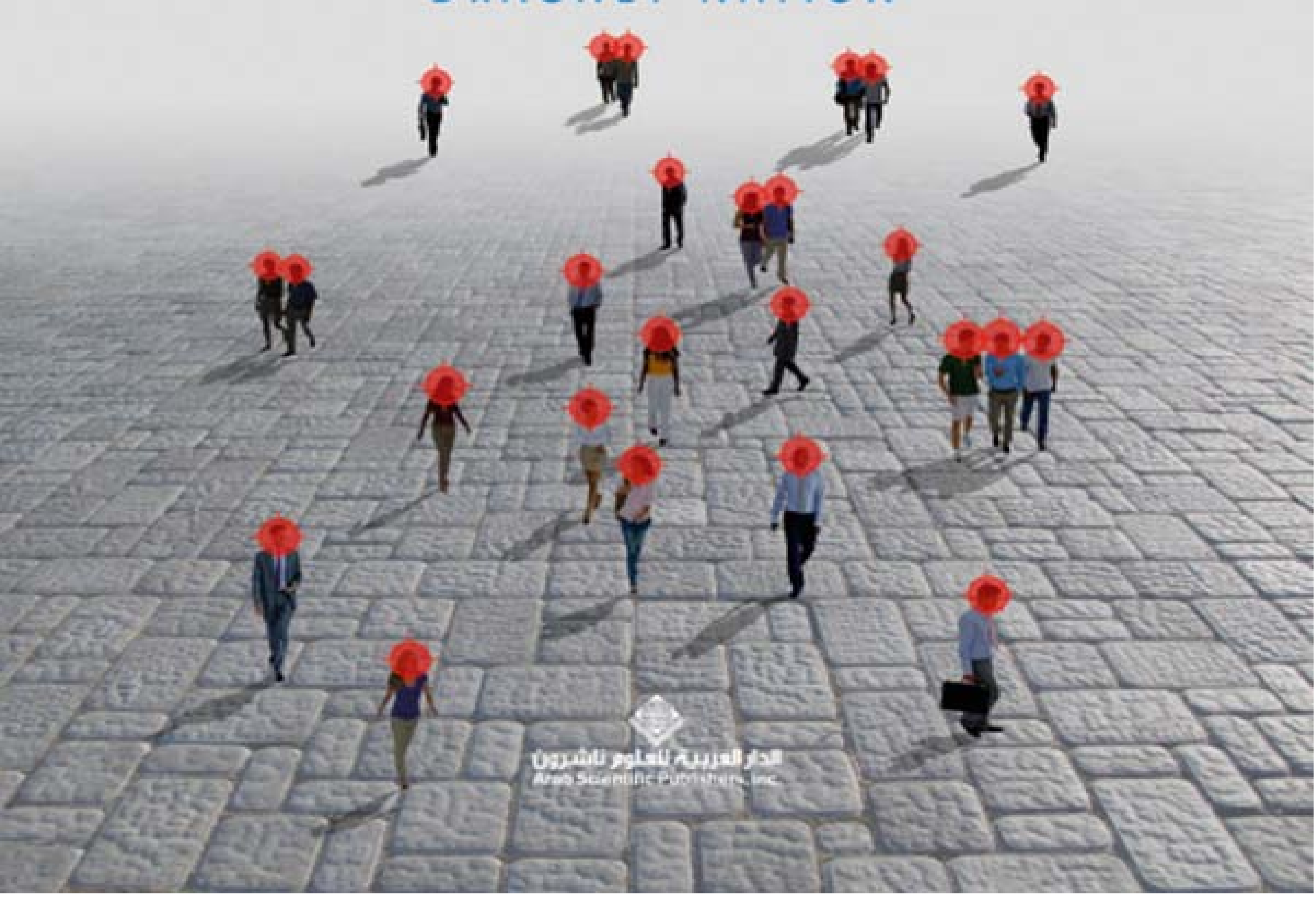
جوليا أنغوين
JULIA ANGWIN

سُلطَة شَبَكات التَعَقُّبْ

عبر وَسَائل الاتّصَال والإنترنت

بَحثٌ عن الخُصوصيَة،
والأمن، والحُريَة في عَالَمٍ رَقَابِيٍّ لا يَستَكين

DRAGNET NATION



سلطة شبكات التعقب عبر وسائل الاتصال والإنترنت

بحث عن الخصوصية، والأمن، والحرية في عالم رقابي لا يستكين

تأليف

جوليا أنغوين

Angwin Julia

ترجمة

حسان البستاني

مراجعة وتحرير

مركز التعريب والبرمجة





يتضمن هذا الكتاب ترجمة الأصل الإنكليزي Dragnet NationA Quest for
Privacy, Security, and Freedom in a World of Relentless
Surveillance حقوق الترجمة العربية مرخّص بها قانونياً من الناشر Times
Books. Henry Holl and Company, LLC بمقتضى الاتفاق الخطي الموقّع
بينه وبين الدار العربية للعلوم ناشرون، ش.م.ل. Copyright © 2014 by
Julia AngwinAll rights reservedArabic Copyright © 2015 by Arab
Scientific Publishers, Inc. S.A.L

الطبعة الأولى
1436 هـ - 2015 م

ISBN: 978-614-02-2493-3

جميع الحقوق محفوظة



عين التينة، شارع المفتي توفيق خالد، بناية الريم
هاتف: (+961-1) 785107 - 785108 - 786233
ص.ب: 13-5574 شوران - بيروت 2050-1102 - لبنان
فاكس: (+961-1) 786230 - البريد الإلكتروني: jchebaro@asp.com.lb
الموقع على شبكة الإنترنت: http://www.asp.com.lb

يمنع نسخ أو استعمال أي جزء من هذا الكتاب بأية وسيلة تصويرية أو الكترونية أو ميكانيكية بما فيه التسجيل الفوتوغرافي والتسجيل على أشرطة أو أقراص مقروءة أو بأية وسيلة نشر أخرى بما فيها حفظ المعلومات،

واسترجاعها من دون إذن خطي من الناشر.

إن الآراء الواردة في هذا الكتاب لا تعبر بالضرورة عن رأي الدار العربية للعلوم ناشرون ش. م. ل

تصميم الغلاف: سامح خلف

التنضيد وفرز الألوان: أبجد غرافيكس، بيروت - هاتف (9611+) 785107
الطباعة: مطابع الدار العربية للعلوم، بيروت - هاتف (9611+) 786233

الفصل الأول
ملفاتكم الكمبيوترية عُرضة للتسلّل

من يراقبكم؟

ذات مرة، كان هذا السؤال يُطرح فقط من قِبَل الملوك، والرؤساء، والشخصيات العامة، الذين يحاولون التملص من الباباراتسي [1] ، ومن قِبَل المجرمين الذين يحاولون الإفلات من القانون. أما سائر الناس فلم يكن التعرض للتعب يقلقهم إلا في مناسبات قليلة.

ولكن السؤال المثير للقلق اليوم - "من يراقب؟" - على صلة وثيقة بالكل بصرف النظر عن شهرته أو شهرتها، أو عن مدى الاقتناع بارتباطه أو ارتباطها بعمل جنائي. يمكن لأي منا التعرّض للمراقبة في أي وقت تقريباً سواءً من قِبَل سيارة تابعة لغوغل ستريت فيو (Google Street View) تلتقط صورة لمنـزلنا، أو من قِبَل مُعلِن يتتبّعنا أثناء تصفّحنا شبكة الانترنت، أو من قِبَل وكالة الأمن القومي التي تتتبّع تفاصيل اتصالاتنا الهاتفية.

اعتادت شبكات التعقُّب التي تغرف معلومات عن كل من تصادفه بدون تمييز أن تكون نادرة؛ كان يتعيّن على الشرطة إقامة حواجز في الطرقات، ولجوء باعة التجزئة إلى تثبيت كاميرات فيديو ومراقبتها. ولكن التكنولوجيا سمحت بظهور عصر جديد من شبكات التعقُّب المعزَّزة يمكنها جمع مقدار كبير من البيانات الشخصية بجهد بشري قليل. إن شبكات التعقُّب تمتد لتطال زوايا أكثر خصوصية من العالم.

تأمّلوا مثلاً بعلاقة شارون جيل وبلال أحمد، وهما صديقان مقرَّبان التقيا على شبكةٍ خاصة للتواصل الاجتماعي تدعى PatientLikeMe.com .

لم يكن بإمكان شارون وبلال أن يكونا أكثر اختلافاً. فشارون والدة وحيدة في الثانية والأربعين من العمر تُقيم في بلدة صغيرة جنوب كنساس. هي تكدح لكسب رِزقها من بيع أغراض منـزلية قيّمة ومستعمَلة في سوق البُرغوث [2] . وبلال أحمد عازب، في السادسة والثلاثين من العمر، مثقَّف ويحمل إجازة من جامعة روتجرز، يُقيم في طابق عُلويّ في سيدني، أستراليا، ويدير سلسلة متاجر محلّية.

بالرغم من عدم التقائهما أبداً شخصياً، أصبحا صديقَين مقرَّبَين على منتدى للتواصل الاجتماعي محميٍّ بكلمة مرور وخاص بالمرضى الذين يعانون

من مشاكل تؤثّر في سلامتهم العقلية. كانت شارون تحاول الإقلاع عن تناول عقاقير مضادة للاكتئاب، وبلال يعاني من القلق والكآبة بسبب فقدان والدته.

من زاويتَي العالم البعيدتَين، تمكّنا من إبهاج أحدهما الآخر. لقد لجأت شارون إلى بلال لأنها شعرت بعدم قدرتها على ائتمان أنسبائها وجيرانها الأكثر قرباً إليها على أسرارها. "أعيش في بلدة صغيرة"، قالت لي شارون. "لا أريد أن تُطلَق أحكام عليّ بسبب هذا المرض العقلي".

ولكن شارون وبلال رُوِّعا عام 2010 عندما اكتشفا أنهما مراقَبان على شبكة التواصل الاجتماعي الخاصة.

بدأ ذلك باختراق. ففي 7 أيار/مايو 2010، لاحظت PatientLikeMe نشاطاً غير عادي في منتدى المِزاج حيث تتسامر شارون وبلال. كان منتسب جديد إلى الموقع يحاول تصفّح أو نسخ كل رسالة من منتديَي المِزاج أو التصلّب المتعدد.

تمكنت PatientLikeMe من صدّ الدخيل وتحديد هويّته: شركة نيلسِن، وهي مؤسسة تُجري أبحاثاً عن وسائل الإعلام في نيويورك، ترصد همسات لزبائنها، بمن فيهم صانعو أدوية. وفي 18 أيار/مايو، وجّهت PatientLikeMe لنيلسِن رسالة توقُّف - و- انقطاع وأبلغت زبائنها بعملية الاختراق. (قالت نيلسِن في وقت لاحق إنها لن تقتحم منتديات خاصة. "إنه أمر اعتبرناه غير مقبول"، قال دايف هادسن، رئيس وحدة نيلسِن المتورطة.

ولكن انعطافاً حدث. لقد اغتنمت PatientLikeMe الفرصة لإبلاغ أعضائها بوجود أحرف طباعية صغيرة لم يلاحظوها ربما عندما سجّلوا أسماءهم في الموقع. فالموقع يبيع أيضاً بيانات عن أعضائه لشركات صيدلانية ومؤسسات أخرى.

كان الخبر خيانة مزدوجة بالنسبة إلى شارون وبلال. لم يكن هناك دخيل يرصدهما فحسب، بل شعرا بالخيبة أيضاً لأنه المكان الذي اعتبراه مساحة آمنة لم يكن كذلك. لقد بدا الأمر كما لو أن أحدهم صوّر لقاءً لمدمنين مجهولي الهوية، فغضب هؤلاء لأن الغاية من تصوير ذلك الفيلم وضعه على شرائط فيديو وبيعها. "شعرتُ بأن خصوصيتي منتهَكة تماماً"، قال بلال.

والأسوأ من ذلك أن أيّاً مما جرى لا يُعتبر غير قانونيّ بالضرورة. فليس للقانون موقف واضح من حالة نيلسِن حتى وإن انتهكت شروط الخدمات التي تقدّمها PatientLikeMe ، لأن تلك الشروط لا تُفرَض على

الدوام بطريقة قانونية. واعتُبر وضع شبكة التواصل الاجتماعي قانونياً تماماً لأن PatientLikeMe أوضحت لأعضائها في الأحرف الطباعية الصغيرة بأنها ستجرف كل المعلومات المرتبطة بهم وتبيعها.

هذا هو العيب المأساوي للخصوصية في العصر الرقمي. فغالباً ما يُعرَّف عن الخصوصية بأنها تحرّر من التدخلات غير المسموح بها. ولكن الكثير من الأمور التي تبدو انتهاكاً للخصوصية يُسمَح بها من خلال أحرف طباعية صغيرة في مكان ما.

ومع ذلك، لم نوافق كلّياً بعد، وبطرقٍ شتى، على هذه التدخلات المسموح بها. إذا كان قيام الشركات بغرف معلومات عن السلامة العقلية للناس أمراً قانونياً، فهل هو مقبول اجتماعياً؟

ربما يكون التنصّت على حديث شارون وبلال مقبولاً اجتماعياً لو كانا تاجرَي مخدرات يخضعان للرقابة بموافقة المحكمة. ولكن هل يكون جرف أحاديثهما، كجزء من شبكة تعقُّب ضخمة تراقب همَسات على شبكة المعلومات، أمراً مقبولاً على الصعيد الاجتماعي؟

تقع شبكات التعقُّب التي تجرف بيانات شخصية بدون تمييز في المنطقة الرمادية تماماً بين ما هو قانوني وما هو مقبول اجتماعياً.

á á á

نحن نعيش في دولة شبكات التعقُّب - عالم تعقُّبٍ غير مميِّز حيث المؤسسات تخزّن بيانات عن أفراد بوتيرة غير مسبوقة. فالقوى نفسها التي حملت لنا التكنولوجيا التي نحبها كثيراً - أداء كمبيوتري قوي لأجهزتنا المكتبية، والأجهزة الحضنية، والأجهزة اللوحية، والهواتف الذكية - تزوّد حركة نشوء التعقُّب غير المميِّز بقوة دافعة.

فقبل أن تصبح أجهزة الكمبيوتر مألوفة، كانت مرتفعة الكلفة ويصعب تعقُّب الأفراد من خلالها، وتحتفظ الحكومات بسجلات عن مناسبات محدَّدة فقط، كالولادة، والزواج، ومِلكية عقارات، والوفاة؛ وتحتفظ الشركات بسجلات عندما يشتري الزبون شيئاً ما ويملأ بطاقة كفالة أو ينضمّ إلى برامج لمكافأة الزبائن المنتظمين. ولكن التكنولوجيا سهّلت على المؤسسات من كل الأنواع الاحتفاظ بسجلات، وبكلفة أقلّ، عن كل لحظة من حياتنا تقريباً.

تأمّلوا بوقائع قليلة سمحت بهذا التحوّل. لقد تضاعفت قوة المعالجة في أجهزة الكمبيوتر كل عامَين تقريباً منذ السبعينات، ممكنةً الأجهزة التي كانت ذات مرة بحجم غُرف كاملة من أن تجد متّسَعاً لها في جَيب

سِروال. ومؤخراً، هَوَت كلفة تخزين البيانات من 18,95 دولاراً للجيغابايت الواحد إلى 1,68 دولاراً عام 2012. ومن المتوقع أن تنخفض الكلفة إلى ما دون دولار واحد بعد سنوات قليلة.

لقد سمح الجمع بين أداء كمبيوتري عالٍ، وأجزاء مكوِّنة أصغر وأصغر، وتخزينٍ رخيص، برفع إمكانية تعقّبٍ غير مميِّز للبيانات الشخصية إلى حدٍّ كبير. ليس كل المتعقِّبين دخلاء، مثل نيلسِن. فمن الدخلاء أيضاً العديد من المؤسسات المفترَض بها أن تكون إلى جانبنا، كالحكومة والشركات التي تربطنا بها أعمال.

بالطبع، يبدو أن أكبر شبكات التعقُّب هي تلك التي تديرها الحكومة الأميركية. فبالإضافة إلى غَرف مقادير كبيرة من الاتصالات الأجنبية، تغرف وكالة الأمن القومي أيضاً سجلات أميركية عن حركة الاتصالات عبر الهاتف والإنترنت، وفقاً لمستندات كشف عنها إدوارد سنودن عام 2013، وهو متعاقد سابق مع وكالة الأمن القومي.

ولكن وكالة الأمن القومي ليست الوحيدة (عِلماً أنها الأكثر فعالية) في إدارة شبكات التعقُّب. فالحكومات في مختلف أنحاء العالم - من أفغانستان إلى زمبابوي - تعتمد تقنية رَقابة تتراوح بين تجهيزات الاعتراض بالجملة والأدوات التي تمكّنها من التسلل عن بُعد إلى أجهزة كمبيوتر الناس وهواتفهم. حتى إن الحكومات المحلية وحكومات الولايات في الولايات المتحدة تعتمد تقنيةَ رَقابة تتراوح بين طائرات بدون طيّار وقارئات لوحات تسجيل مؤتمَتة تمكّنها من مراقبة تحركات المواطنين بطرق لم تكن ممكنة من قَبل. وتتعقّب الشرطة المحلّية الناس باطّراد من خلال استخدام إشارات تبثّها هواتفهم المحمولة.

في غضون ذلك، تزدهر شبكات التعقُّب التجارية للقبض على مطلوبين. فـأيه تي أند تي وفِريزون تبيعان معلومات عن مواقع زبائنهما الذين يستخدمون هواتفهما المحمولة، ولكن دون تحديد هويّتهم. وشرع مالكو مراكز التسوّق باعتماد تقنيّةٍ لتعقّب المتسوّقين من خلال إشارات تبثّها الهواتف المحمولة في جيوبهم. لقد استخدم باعة التجزئة مثل هول فودس إشارات رقمية هي في الواقع أجهزة مسح لتمييز الوجوه. وتستخدم بعض وكالات البيع خدمةً من داتايوم (Dataium) تسمح للوكالات بمعرفة السيارات التي قمتم بتصفّحها عبر الإنترنت، إذا أرسلتم لها عنوان بريدكم الإلكتروني، وذلك قبل وصولكم إلى مكاتب وكيل البيع.

عبر الإنترنت، يعمد مئاتُ المعلِ نين ووسطاء البيانات إلى مراقبتكم

أثناء قيامكم بتصفّح شبكة المعلومات. فببحثكم عن معلومات حول نسبة السكّر في الدم يمكن أن تُعتبروا مرضى محتمَلين بداء السكّري من قِبَل شركات تضع نِبْذات عن الناس استناداً إلى حالتهم الطبّية، ومن ثم تمكين شركات الأدوية والمؤمِّنين من ولوج تلك المعلومات. ويمكن للبحث عن حمّالة صدر أن تُشعل حرب عروض فَورية بين المعلِنين عن ملابس داخلية نسائية في أحد مواقع المزاد العلني عبر الإنترنت.

وهناك تقنيات تعقُّب جديدة وشيكة: تضيف شركات إلى الهواتف والكاميرات تقنيّةً لتمييز الوجوه؛ وتُضاف إلى السيارات تقنية لمراقبة موقعكم؛ وتُطوَّر أجهزة لاسلكية ذكية تقيس استخدام الطاقة الكهربائية في منـزلكم؛ وطوّر محرِّك البحث غوغل غلاس ، وهي كاميرات بالغة الصِّغر مبيَّتة في نظارات تسمح للناس بالتقاط صور وتصوير أفلام فيديو دون رفع إصبع واحدة.

á á á

يقول المتشككون: أين الخطأ إذا قام مراقبون غير مرئيّين بجمع كل بياناتنا؟ من الذي تأذّى؟

من المعترَف به صعوبة إثبات حدوث أذى شخصي جرّاء خرق للبيانات. فلو حُرِمت شارون أو بلال من وظيفة أو تأمين، لما عرفا ربما أيَّ جزء من البيانات تسبّب بالحرمان. فالأشخاص الذين تمنعهم الحكومة الأميركية من الصعود على متن طائرة تجارية للسفر داخل الولايات المتحدة أو خارجها لا يبلَّغون أبداً بالبيانات التي ساهمت في القرار.

ولكن الجواب بسيط على النطاق الأوسع: يمكن إساءة استعمال مجموعات قيّمة من البيانات الشخصية، وسيُساء استعمالها حكماً.

تأمّلوا إحدى أقدم شبكات التعقُّب، غير المؤذية كما هو مُفترَض: الإحصاء الأميركي. فالقانون يحمي خصوصية المعلومات الشخصية التي يجمعها الإحصاء، ولكن الإحصاء تعرّض لسوء الاستعمال تكراراً. لقد استُخدم في الحرب العالمية الأولى لتحديد مواقع المتهرّبين من الخدمة العسكرية. وفي الحرب العالمية الثانية، زوّد مكتب الإحصاء إدارة الاستخبارات الأميركية بأسماء وعناوين المقيمين الأميركيين من أصل ياباني؛ لقد استُخدمت المعلومات لجمع المقيمين اليابانيين ووضعهم في معسكرات اعتقال. لم يُصدر مكتب الإحصاء اعتذاراً رسمياً عن سلوكه إلا في العام 2000. وفي عامَي 2002 و2003، زوّد مكتب الإحصاء وزارة الأمن الداخلي بمعلومات إحصائية عن الأميركيين من أصل عربـي. وبعد الدعاية السيّئة التي تعرّض لها المكتب،

أعاد النظر بسياساته وبات الحصول على معلومات حسّاسة كالعِرق، والإثنية، والدين، والانتساب السياسي، والتوجّه الجنسي، رهناً بموافقة مسؤولين رفيعي الرُّتَب.

ليست الولايات المتحدة الوحيدة في إساءة استعمال الإحصائيات السكانية. لقد استخدمت أستراليا بيانات القَيد السكانية لإرغام السكان الأصليين على الهجرة عند منقلَب القرن العشرين. في جنوب أفريقيا، كان الإحصاء وسيلة أساسية لسياسة التمييز العنصري المتّبَعة من قِبَل الدولة. وأثناء الإبادة الجماعية الرواندية عام 1994، استُهدف الضحايا التوتسي من خلال بطاقات الهويّة التي تشير إلى إثنيّتهم.

غالباً ما يساء استعمال البيانات الشخصية لأسباب سياسية. وإحدى الحالات السيئة السُّمعة برنامجٌ يدعى كوينتلبرو قام بتنفيذه مكتب التحقيقات الفيدرالي (أف بـي آي) في أواخر الستينيات. لقد وضع مدير الأف بـي آي - جيه. إيدغار هوفر - البرنامج السرّي للتجسس على مخرِّبين ومن ثم استخدام المعلومات لمحاولة تشويه سمعتهم وإثباط عزيمتهم. وذهبت الأف بـي آي بعيداً بالغةً حدّ إرسال شريط لمارتين لوثر كينغ الابن يحمل تسجيلاً ناجماً عن إخضاع غرفة فندقه للرَّقابة، وأُريدَ منه التسبب بانفصال كينغ عن زوجته، مع رسالة قصيرة اعتبرها كينغ تهديداً له بالكشف عن التسجيل.

ووجد المتسللون الجانون أيضاً أن استخدام بيانات شخصية هو الطريقة الفضلى لخرق دفاعات مؤسسة ما. تأمّلوا بكيفية قيام المتسللين الصينيين باختراق أر أس إيه الرائدة في الأمن الكمبيوتري المتطوّر. لقد ألقى المتسللون طُعماً لمواقع تواصل اجتماعي بهدف الحصول على معلومات عن موظفين فرديين. بعد ذلك، أرسلوا لهؤلاء الموظفين بريداً إلكترونياً بعنوان **مخطط التجنيد للعام *2011*** . بدا البريد الإلكتروني قانونياً بما يكفي لدرجة قيام أحد الموظفين بسحبه من ملفٍّ بريدٍ تلقائي (junk mail) وفتْحه. فأدخل ذلك الملف برنامجاً تجسسياً لجمع المعلومات على جهاز الموظف، ومن هناك تمكن المهاجمون من دخول عدة أجهزة في المؤسسة من خلال التحكّم عن بُعد.

باختصار، لقد تسللوا إلى ملفات كمبيوترية عائدة لأشخاص لا لمؤسسات.

لا يقتصر التسلل إلى ملفات الأشخاص على المجرمين فقط. فالمسوّقون يلاحقوننا في كل مكان على شبكة الانترنت أملاً في تمكنهم من الحصول

على معلومات تسمح لهم بالتسلل إلى ملفاتنا الكمبيوترية لحملنا على شراء منتجاتهم. وتغرف وكالة الأمن القومي كل اتصالاتنا الهاتفية لوضع أنماط تعتقد أنها تسمح للسلطات بالتسلل إلى ملفات خليّة إرهابية.

في ما يلي بعض الوقائع التي تشير إلى إمكانية التسلل إلى ملفاتكم:

1 يمكن العثور عليكم على الدوام.

- يمكن مراقبتكم في منـزلكم - أو في الحمّام.
- لم يَعُد بإمكانكم الاحتفاظ بسرّ.
- يمكن انتحال شخصيّتكم.
- يمكنكم الوقوع في شرَك جدار مرايا .
- يمكن التلاعب بكم مالياً.
- يمكن وضعكم في طابور لتمييز الوجوه في مركز للشرطة.

هذه القائمة ليست شاملة بل مستوحاة من أحداث الحياة اليومية في الوقت الحاضر. في المستقبل، سيكون بإمكاننا على الأرجح قراءة هذه القائمة والسخرية من كل الأشياء التي أخفقتُ في تخيّلها.

يمكن العثور عليكم على الدوام

يخزَّن اسمكم، عنوانكم، وتفاصيل أخرى محدِّدة للهوية - لا بل موقعُ هاتفكم المحمول أيضاً في أي وقت - في قواعد بيانات متنوّعة لا يمكنكم ولوجها أو التحكم بها. فالمختلِسون والموظفون الخبثاء يجدون باطّراد طرقاً لإساءة استعمال قواعد البيانات هذه.

ففي العام 1999، استأجر رجل مخبول خدمات وسيط بيانات عبر الإنترنت يدعى دوكوسيرتش بهدف العثور على رقم ضمان اجتماعي، ومعلومات توظيف، وعنوان منـزل امرأة تستحوذ على عقله تدعى آمي بويِر. بعد أيام قليلة، توجّه يُونـز بسيارته إلى مقر عمل بويِر وأطلق عليها النار وقتلها أثناء مغادرتها المكان. بعد ذلك، انتحر بطلق ناريّ.

قاضت عائلة بويِر وسيط البيانات، ولكن المحكمة العليا في نيو هامبشير اعتبرت أنه في حين يتعيّن على وسيط البيانات "إيلاء عناية معقولة" أثناء بيع بيانات شخصية، "يمكن ملاحظة معلومات كعنوان مقر العمل بسهولة من قِبَل أفراد المجتمع، ولا يمكن للعنوان أن يكون خاصاً".

لم يحقق أهل بويِر إلا القليل: عام 2004، توصّلوا إلى تسوية مع دوكوسيرتش لقاء 85,000 دولار بعد سنوات مُرهِقة من المعارك القانونية. وما تزال دوكوسيرتش تمارس عملها المعتاد، وما يزال موقعها يروّج لخدمات تتضمن بحث عكسيّ عن رقم هاتف. بحث عن لوحة تسجيل. العثور على

رقم ضمان اجتماعي. وبحث عن حساب مصرفي مخبَّأ.

مذاك الحين، انخفض ثمن شراء عناوين أشخاص من نحو 200 دولار دفعها يُونِـز إلى 95 سنتاً لقاء تقرير كامل عن الفرد. وأصبحت حالات اقتفاء الأثر عن بُعد عبر شبكة المعلومات مألوفة جداً لدرجة أنها نادراً ما تُعتبر خبراً يستحق النشر.

تأمّلوا بمثل واحد فقط. في العام 2010، أُدين نائب عُمدة ساكرامنتو، تشو فو، بارتكاب جريمة قتل بعد إطلاقه النار على ستيف لو وقتله، وكان لو على علاقة غرامية بزوجة فو. أثناء المحاكمة، تبيّن أن فو بحث عن اسم لو في قاعدة بيانات إنفاذ القانون، وطلب من أحد زملائه البحث عن لوحة تسجيل لو، وعثر على عنوان لو من خلال خدمة هاتفية عبر الإنترنت. حُكم على فو بالسجن مدى الحياة دون إطلاقِ سراحٍ مشروط.

ويمكن أيضاً إساءة استعمال البيانات الأكثر براءة؛ مثل سجلات الرحلات الجوّية. ففي العام 2007، اتُّهم موظف في وزارة التجارة، يدعى بنيامين روبنسون، بولوج قاعدة البيانات الحكومية بشكل غير قانوني أكثر من 163 مرة، وهي التي تحتوي على السجلات الدولية لحجوزات الرحلات الجوّية. فبعد انقطاع علاقته بامرأة، ولج ملفاتها وملفات ابنها الصغير وزوجها، وترك رسالة على مُجيبها الآلي تُفيد بأنه سيتحقق من الملفات "لأرى إذا كنت تكذبين في شأن أي أمر"، وأوحى أنه قد يتمكن من ترحيلها. في العام 2009، اعترف روبنسون بذنبه بالحصول على معلومات بشكل غير قانوني من جهاز كمبيوتر مَحميّ، وحُكم عليه بالخضوع للمراقبة لمدة ثلاث سنوات.

إن اليوم الذي يصبح فيه التعقّب الحالي روتينياً ليس ببعيد. فالولايات المتحدة تُضمِّن جوازات السفر شرائح لتحديد الترددات الراديوية (RFID) يمكنها نقل بيانات على مسافة قصيرة تبلغ نحو عشرة أقدام، ويشرع المستخدِمون والمدارس بوضع الشرائح في بطاقات الهويّة. ففي العام 2013، رفض قاضٍ فيدرالي في تكساس اعتراض طالبة على الإجراء الذي اتخذته مدرستها بوجوب تقلّد بطاقة تعريف مزوَّدة بشريحة لتحديد الترددات الراديوية. حتى إن بعض المستخدِمين تعاطفوا مع فكرة غرس الشرائح تحت بشرة مستخدَميهم، مما حدا بكاليفورنيا إلى تحريم هذه الممارسة عام 2008.

وأصبح تعقّب الهواتف المحمولة أمراً روتينياً في أقسام الشرطة. ففي العام 2011، تقدّمتُ وزميلي في وول ستريت جورنال ، سكوت ثارم، إلى الولايات العشرين الأكبر وأقسام الشرطة المحلية في الولايات المتحدة بطلبات للحصول على سجلات مفتوحة. فوفّرت ثماني وكالات إحصائياتٍ موجَزة على

الأقل توحي بقيام الوكالات المحلية وعلى مستوى الولايات بتعقُّب آلاف الهواتف المحمولة كل عام تُجرى من خلالها اتصالات حالية. فالأمر روتينيّ بقدر "البحث عن دليل من خلال بصمة إصبع أو دي أن أيه"، قال غريغ روسمان، وهو نائب عام في مقاطعة بروارد، فلوريدا.

كان من الحتميّ شروع شركات الهواتف ببيع بيانات مواقع الهواتف المحمولة لجمهور أوسع من الشرطة. ففي العام 2013، قالت فِريزون إنها ستبيع منتجاً جديداً يدعى برِسيجن ماركت إينسايتس يسمح للمؤسسات بتعقّب مستخدمي الهواتف المحمولة في مواقع محدَّدة.

وأحد أول زبائن فِريزون فريق كرة القدم فينيكس صنـز الذي يريد معرفة مكان إقامة أنصاره. وقال سكوت هورويتز، نائب رئيس الفريق: "إنها المعلومات التي أرادها الجميع والتي لم تتوافر حتى الآن".

يمكن مراقبتكم في منزلكم - أو في الحمّام

عام 2009، واجهتْ مساعدةُ مدير مدرسة ثانوية الطالبَ بلايك روبينـز البالغ من العمر خمسة عشر عاماً، مدّعيةً أنها تملك دليلاً على "اعتماده سلوكاً غير مناسب في منـزله". وتبيّن أن مدرسته - ثانوية هاريتون الواقعة في منطقة إدارة مدارس ميسورة في ضواحي فيلادلفيا - وضعت برنامج تجسّس على أجهزة أبل ماك بوك الحضنية العائدة لألفَين وثلاثمئة طالب. كان تقنيّو المدرسة قد فعّلوا البرنامج على بعض الأجهزة الحضنية، وبات بإمكانهم التقاط صور فوتوغرافية من خلال كاميرا الويب، إضافة إلى التقاط صور لشاشات أجهزة كمبيوتر الطلاب. لقد أخذت كاميرا الويب بلايك على حين غَرّة حاملاً أشياء على صورة حبّة دواء. فقال بلايك وعائلته إنها سكاكر مايك أند آيك. ولكن مساعدة المدير كانت على ثقة بأنها مخدرات.

قاضت عائلة بلايك إدارة المدارس بتهمة انتهاك خصوصية ابنها. وقالت المدرسة إن البرنامج وُضع للسماح للتقنيين بتحديد موقع أجهزة الكمبيوتر في حال تعرّضها للسرقة. ولكن المدرسة لم تُبلغ الطلاب بوجود البرنامج، كما أنها لم تضع توجيهات حول الوقت الذي يقوم فيه الموظفون التقنيون بتشغيل الكاميرات.

وأظهر تحقيق داخلي أنه تم تفعيل الكاميرات على أكثر من أربعين جهازاً حضنياً، والتُقطت أكثر من خمسة وستين ألف صورة. والتُقطت صور لبعض الطلاب آلاف المرات ولا سيما عندما كانوا متعرّين جزئياً ونائمين. وقال طالب سابق، ويدعى جوشوا لِفين، إنه "صُدم وشعر بالإذلال وبكَرَب عاطفيّ شديد" عندما رأى بعضاً من الصور الفوتوغرافية الثمانية آلاف التي

التُقطت عبر كاميرا الويب وشاشة جهازه الحضني. قاضى لِفين، روبينـز، وطالب آخر، المدرسةَ وفازوا بتسوية مالية. ومنع مجلس الإدارة المدرسة من استخدام الكاميرات لمراقبة الطلاب.

نحن معتادون على فكرة وجود كاميرات للرَّقابة في كل مكان. ويُقدَّر وجود أكثر من أربعة آلاف كاميرا للرَّقابة في مانهاتن السفلى. وتشتهر لندن بكاميرات للرَّقابة الأمنية يفوق عددها الخمسمئة ألف.

ولكن مع غدوّ الكاميرات أصغر حجماً، بات بإمكانها التجوّل داخل منازلنا وأماكننا الحميمة، مُربِكةً تعريفاتنا للعام والخاص. وأصبحت الطائرات بدون طيار المزوَّدة بكاميرات رخيصة بما يكفي لتشكل مصدر إزعاج. ففي أيار/مايو 2013، شكت امرأة من سياتل على مدوَّنة محلية: "قام رجل غريب بإطلاق طائرة فوق فنائي وبجانب منـزلي... لقد أوحى لي الأزيز الصخّاب في بادئ الأمر بأنها أداة لإزالة الأعشاب الضارّة في هذا اليوم الربيعي الدافئ". عندما فاتح زوجها الرجل الذي يطلق طائرة بدون طيار بالأمر، قال إن القانون يسمح له بذلك وإنها مزوَّدة بكاميرات. وأضافت المرأة: "نحن شديدو القلق لأنه يمكن أن يكون بسهولة تامة مجرماً يخطط لاقتحام منـزلنا أو استراق النظر".

في ظل هذه التكنولوجيا الجريئة، ينشئ الأشرار بالطبع شبكات تعقُّب خاصة بهم مزوَّدة بكاميرات. ففي العام 2013، وصف الصحافي نيت أندرسون مجموعةً قوية من المتسلّلين إلى ملفات كمبيوترية تتّجر بأفكار مفيدة وتقنياتٍ لوضع برنامج تجسسي في كاميرات ويب عائدة لنساء بهدف جمع معلومات. "يعملون علَناً عبر الإنترنت، متشاطرين أفضل التقنيات"، كتب. "ودعوة معظم هؤلاء الأشخاص متسلِّلون يشكل ضرراً حقيقياً في كل مكان للمتسلِّلين؛ المطلوب الآن مهارة تقنية بالحد الأدنى لا غير".

عام 2011، أُدين رجل في سانتا آنا يدعى لويس ميجانغوس بالتسلل إلى ملفات كمبيوترية والتنصّت على الهاتف بعد اكتشاف استخدامه برنامجاً ماكراً يسمح له بالتحكم بكاميرات ويب عائدة لأكثر من مئة كمبيوتر. في إحدى الحالات، تحكم بكاميرا ويب عائدة لمراهقة وحصل على صور فوتوغرافية لها تبدو فيها عارية. واستخدم الصور لابتزاز ضحاياه والحصول على صور إضافية تظهرنَ فيها عاريات. أثناء الحكم، قال القاضي: "لا يمكن وصف الأمر إلا بكونه جهداً متواصلاً لترهيب الضحايا". حُكم على ميجانغوس بالسجن لمدة ست سنوات.

فشبكات التعقُّب عبر الكاميرات الواسعة الانتشار موجودة وراء كل

زاوية. ووصول أجهزة كمبيوتر مزوَّدة بكاميرات، مثل نظارات غوغل، يعني أن كل شيء قابل للتصوير. لقد صُدم المحرر الصحفي في نيويورك تايمز ، نيك بيلتون، عندما حضر ندوة لغوغل ووجد أن عدداً من الحاضرين يضعون نظارات غوغل المزودة بكاميرات أثناء استخدامهم للمباول.

ولكن المتحمسين لنظارات غوغل يقولون إن وضع كاميرات على رؤوسهم يغيّر حياتهم. "لن أعيش يوماً من حياتي من الآن فصاعداً بدونها (أو بدون منافِس)"، كتب المدوِّن روبرت سكوبل بعد اختبار النظارة لمدة أسبوعَين. "يعتبرها بعض الأشخاص أمراً مزعجاً"، اعترف، ولكنه قال، "إنها جديدة وستنفذ الكميات المعروضة عندما تنـزل إلى السوق".

لم يَعُد بإمكانكم الاحتفظ بسرّ

حاولت بوبـي دنكان، وهي طالبة ذات ميول جنسية غير سوية في الثانية والعشرين من العمر في جامعة تكساس، أوستن، إخفاء ميولها عن عائلتها. ولكن فيسبوك فضح أمرها بطريقة غير متعمَّدة عندما أضافها رئيس جوقة غير الأسوياء جنسياً في الحرم الجامعي إلى مجموعة المناقشة على فيسبوك. لم تكن بوبـي تعرف أن باستطاعة صديقٍ ضمَّها إلى مجموعة ما بدون موافقتها، ومن ثم قيام فيسبوك بتوجيه رسالة قصيرة لقائمتها الكاملة من الأصدقاء - بمن فيهم والدها - لإبلاغهم بانضمامها.

بعد يومَين من تلقّي خبر انضمام بوبـي إلى جوقة غير الأسوياء جنسياً ، كتب والدها على صفحته في فيسبوك: "لكم كلكم أيها غير الأسوياء أقول، عودوا إلى مساكنكم القذِرة وانتظروا.... الجحيم ينتظر ضلالكم. حظاً سعيداً أثناء غنائكم الجماعي هناك".

لدى إبلاغه بالحالة، قال الناطق بلسان فيسبوك، أندرو نويس، إن "الاختبار المشؤوم يذكّرنا بأنه يجب علينا مواصلة عملنا لمساعدة المستخدِمين وتثقيفهم حول وسائل الضبط القوية التي نعتمدها للحفاظ على الخصوصية". لقد بدا موقفه إلقاءً باللوم على الضحية بسبب استخدامها الفيسبوك بطريقة خاطئة. ولكن لم يكن هناك على فيسبوك ما يمكن لبوبـي الاستعانة به للحؤول دون انضمامها إلى المجموعة بدون إذنها.

"أُلقي اللوم على فيسبوك"، قالت بوبـي. "لا يُفترض أن يكون ما يراه الناس مني خيارَ شخص آخر سواي".

وبجرف مزيد من البيانات الشخصية إلى داخل قواعد بيانات متنوعة، ازدادت صعوبة الاحتفاظ بأي سرّ - حتى من قِبَل المؤتَمَنين على الأسرار. والمثال الأبرز هو مدير السي آي أيه، ديفيد بتريوس، الذي استقال بعد أن

كشف تحقيقٌ غير ذي صلة أجرته الأف بـي آي النقابَ عن رسائل موجَّهة بالبريد الإلكتروني تشير إلى انخراطه بعلاقة غرامية خارج الزواج. وفي العام 2002، أُدين المحلل السابق في السي آي أيه، جون كيرياكو، بتمرير معلومات سرّية لصحافيين بالاستناد جزئياً إلى بريد إلكترونيّ اعتُبر دليلاً. فاعترف بذَنْبه وحُكم عليه بالسجن لمدة ثلاثين شهراً.

حتى إنه يصعب الاحتفاظ بالأسرار الصغيرة. فالأشخاص الذين يحمّلون أجهزتهم الكمبيوترية أفلاماً إباحية استُهدفوا من قِبَل ما يُدعون مُنفِذي حقوق النشر الذين يتقدّمون بدعاوى قضائية جماعية تسمح لهم بالحصول على معلومات عن هويّات الأشخاص الذين حمّلوا أجهزتهم، من خلال شبكات مشاطرة الملفات، أفلاماً خلاعية تحميها حقوق النشر، وذلك بهدف إحراج المدّعى عليهم كي يتمّ التوصل إلى تسوية مالية سريعة.

وفي تموز/يوليو 2012، أجازت محكمة الاستئناف الأميركية للدائرة الخامسة النظر في قضية مماثلة تقدّم بها محامي منتجِ أفلامٍ سينمائية للبالغين كان قد قاضى 670 شخصاً حمّلوا أجهزتهم أفلاماً يملك المنتج حقوق نشرها، وذلك بالاستناد إلى عناوين أجهزتهم، وسعى للحصول على هويّاتهم دون موافقة المحكمة. وصفت المحكمة "انتهاكات المحامي محاوَلةً لتكرار استراتيجيته بمقاضاة مستخدمين مجهولي الهوية لشبكة الإنترنت يزعم أنهم حمّلوا أجهزتهم أفلاماً بطريقة غير قانونية، مستخدماً سلطات المحكمة للعثور على هويّاتهم، ومن ثم حملهم على الشعور بالخجل والتهويل عليهم بهدف التوصل إلى تسوية مالية تقدَّر بآلاف الدولارات".

وفي أيار/مايو 2013، ذهب قاضٍ في كاليفورنيا بعيداً، معلِناً أن مُنفِذي حقوق النشر استخدموا "مجموعة مترابطة من قوانين حقوق نشر قديمة العهد، واختلافاً اجتماعياً مُصيباً بالشلل، وتكاليف دفاع لا يمكن تحمّلها، كي ينهبوا المواطنين".

يمكن انتحال شخصيّتكم

أُخذت جاليزا سويل من والدتها ووُضعت قيد الحضانة (دار رعاية داخلية) عندما كانت في الثامنة من العمر. لقد وُضعت في سبعة دور احتضان مختلفة قبل أن تغادر نظام الحضانة. عندما بلغت الحادي والعشرين من العمر وكانت على وشك التخرج من جامعة جورج واشنطن، تقدّمت بطلب للحصول على بطاقة ائتمان. عندئذٍ، اكتشفت أن إحدى أفراد عائلتها سرقت شخصيّتها، وحصلت على بطاقة ائتمان باسمها، وتخلّفت عن تسديد الدَّفعات المالية.

بدون القدرة على الاستدانة، لا يمكن لجاليزا الحصول على سيارة، فشعرت بالقلق من عدم تمكّنها من امتلاك شقة بعد التخرج. "غالباً ما أجد نفسي قلقة مما إذا كنت سأحصل على مكان للإقامة فيه في اليوم التالي أو الحصول على طعام، وقد عملتُ بكدّ للحرص على عدم حدوث ذلك، كما تعلمون، بعد إعتاقي"، قالت لمشاركين في حلقة تدريب تتناول موضوع سرقة الهويّة عام 2011. "ولكنني أجد نفسي الآن في ذلك الوضع الدقيق لسبب بسيط ألا وهو عدم حصولي على خط ائتمان".

من المؤسف أن يكون أطفال الحضانة مثل جاليزا من بين الضحايا الأكثر شيوعاً لجريمة سرقة الهويّة. أفضّل دعوة الجريمة انتحال شخصية ، لأن أحداً لا يمكنه سرقة هويّتك في الواقع. فجاليزا ما تزال نفسها. لقد انتحل شخص ما شخصيتها ببساطة بهدف تحقيق كسب ماليّ.

استجابةً للمشكلة المتفاقمة المتمثلة بانتحال شخصية أطفال الحضانة، وقّع الرئيس باراك أوباما قانوناً عام 2011 يتضمّن بنداً يشترط قيام الشركات التي تراقب الوضع الائتماني للأفراد والمؤسسات بتزويد أطفال الحضانة بتقرير ائتمانيّ مجّاني سنويّ بعد بلوغهم سنّ السادسة عشرة ما داموا منتسبين إلى نظام الحضانة.

ولكن المشكلة الضمنية لانتحال الشخصية تستفحل باطّراد. لقد ازدادت شكاوى سرقة الهويّة بمعدّل الثلث تقريباً عام 2012 - ارتفعت عائدات السرقات من 279 مليون دولار عام 2011 إلى 369 مليون دولار عام 2012 - بعد استقرارٍ نوعاً ما في السنوات الخمس السابقة، وفقاً لإحصائيات لجنة التجارة الفيدرالية.

كان الاحتيال المرتبط بسرقة بطاقات الائتمان الشكوى الأكثر شيوعاً، وفقاً لستيف توبوروف، محامي لجنة التجارة الفيدرالية الذي ينسّق برنامج الوكالة لحماية الشخصية. في هذه الأيام، قال ستيف: "إن الاحتيال الضريبي هو في رأس قائمة الشكاوى". وتابع: "نرى أيضاً أشكالاً جديدة من الاحتيال، كالاحتيال الطبي حيث يستخدم الناس معلومات شخصية للحصول على علاج صحّي". يصعب على الناس اكتشاف الاحتيال الضريبي والطبي لأنهم لا يستطيعون ولوج ملفاتهم بسهولةِ ولوجِ التقارير الائتمانية.

عام 2013، أُدينت امرأتان فلوريديّتان بالاحتيال على الحكومة عندما قدّمتا ألفَي إقرار ضريبي احتيالي لدائرة الإيرادات الداخلية بهدف استرداد 11 مليون دولار. دفعت وزارة الخزانة نحو 3,5 مليون دولار. لقد أعدّت إحدى المرأتَين، وتدعى آلسي بوناني، العديد من الإقرارات الضريبية الاحتيالية

من خلال استخدام معلومات اشترتها من ممرّضة مستشفى. وأعلن المستشفى، باتيست هيلث ساوث فلوريدا، أنه تمّ ولوج 834 سجلّ مريض. قال موظف في دائرة الإيرادات الداخلية، ويدعى توني غونـزاليس، لمحطة تلفزيونية محلية إن "الاشرار القادرين على الحصول على أرقام الضمان الاجتماعي هذه يشترونها من موظفين يعملون في هذه المستشفيات والمراكز الطبية، وتباع بـ150 دولاراً للرقم الواحد".

لا تتمّ سرقة معلومات شخصية فحسب، بل تضيع في كل الأوقات أيضاً لأسباب تتراوح بين الإهمال والتسلل إلى ملفات كمبيوترية. كانت التقارير الحكومية عن خروقات للبيانات في تزايد مطّرد منذ العام 2009، وقفزت بنسبة دراماتيكية بلغت 43 بالمئة عام 2012، وفقاً لموقع DataLossDB التابع لـمؤسسة الأمن المفتوح .

نادراً ما تعاقَب الشركات على فقدان بياناتٍ خاصة بالزبائن، وهناك قضية نموذجية ذات أثر غير مسبوق نجمت عن تسللات متكررة إلى ملفات كمبيوترية في سلسلة فنادق ويندهام. ففي العام 2008، اقتحم متسللون شبكة أجهزة كمبيوتر فندق ويندهام في فينيكس. ومن خلال تلك الشبكة، تمكن المتسللون من ولوج حسابات البطاقات الائتمانية لأكثر من خمسمئة ألف زبون في فنادق ويندهام الواحد والأربعين، ونقلوا المعلومات إلى روسيا. لقد جمع المتسللون، كما زُعم، مبلغ 10,6 مليون دولار.

ولكن ويندهام أخفقت في ضمان أمن شبكتها الكمبيوترية حتى بعد ذلك الخَرق، وتمّ التسلل مجدداً إلى ملفاتها في العام التالي، فاقدةً على التوالي خمسين ألف وتسع وستين ألف بطاقة ائتمان خاصة بزبائنها. وفي العام 2012، قاضت لجنة التجارة الفيدرالية ويندهام، زاعمةً أن إخفاقها في ضمان أمن شبكتها كان مضلِّلاً وجائراً بالنسبة إلى الزبائن.

فردّت ويندهام، مدّعيةً أن لجنة التجارة الفيدرالية عاقبت الشركة بطريقة جائرة كونها ضحية جريمة، معتبرةً القضية "مماثلة لمعاقبة مستودع الأثاث المحلّي بسبب تعرّضه للسرقة والإغارة على ملفاته". أجابت لجنة التجارة الفيدرالية أن "هناك مشابَهة أكثر دقة تكون فيها ويندهام مستودع أثاث محلّي ترك نسخاتِ معلوماتٍ عن بطاقات الائتمان وبطاقات الخصم الخاصة بزبائنها على المنضدة، وقصّرت في إقفال أبواب المتجر في الليل، وصُدمت عندما وجدت في الصباح أن هناك من سرق المعلومات".

يمكنكم الوقوع في شرَك جدار مرايا

تقول الشركات التي تراقب سلوك متصفّحي شبكة الإنترنت إن أعمالهم

آمنة: يريدون فقط أن يحملوا أشخاصاً أنعموا النظر مؤخراً بالأحذية على رؤية دعايات أحذية، أو يحملوا أشخاصاً يفضّلون أخباراً سياسية على رؤية أخبار سياسية. أدعو هذا النوع من الترويج الجماعي وفقاً لطلب الزبون جدار مرايا .

يكون جدار المرايا مفيداً أحياناً. لا أمانع بصفة خاصة رؤية إعلان يذكّرني بشراء مُنتَج كنت أُنعم النظر به. ولكن جدار المرايا قد يدخل أيضاً مجالاً مزعجاً.

تأمّلوا بما يلي: وفقاً لدراسة أجرتها الأستاذة الجامعية في هارفارد، لاتانيا سويني، في كانون الثاني/يناير 2013، يولّد البحث عن اسم يوحي بأن حامله شخص أسود، مثل تريفون جونـز، دعايات توحي على الأرجح بمدوَّنة اعتقال - مثل "تريفون جونـز اعتُقل؟" - أكثر بنسبة 25 بالمئة مما يولّده البحث عن اسم يوحي بأن حامله شخص أبيض مثل "كريستن سبارو". ووجدت سويني أن هذا التفاوت الدعائي بالنسبة إلى الأسماء قائم أيضاً عندما يكون لدى الشخص الذي يحمل اسماً يوحي بأنه أبيض سجلاًّ جنائياً، ولا يكون لدى الشخص الذي يحمل اسماً يوحي بأنه أسود سجلاًّ جنائياً.

وتُستخدم البيانات المرتبطة بسلوك متصفّحي شبكة الإنترنت أيضاً، وبشكل متزايد، لتوفير ما يُدعى محتوى وفقاً لطلب الزبون. على سبيل المثال، تستخدم غوغل معلومات من أبحاث سابقة وعاداتٍ تصفّحية لتوفير نتائج بحث مختلفة لأشخاص مختلفين؛ حتى عندما يُجرون أبحاثاً مماثلة. أحياناً، تكون تلك الاستكمالات مفيدة، كما هو الحال عندما تقترح غوغل مطعماً قرب مكان إقامتك بدلاً من اقتراح مطعم في مكان بعيد. ولكن الاستكمالات تكون متطفِّلة أحياناً.

ففي الأشهر السابقة لانتخابات تشرين الثاني/نوفمبر 2012 الرئاسية، وضعت غوغل تخمينات مثيرة للجدل في الشأن السياسي. لقد رأى الباحثون عن باراك أوباما أخباراً عن الرئيس متداخلة مع عمليات بحث مستقبلية عن مواضيع أخرى. ولم يرَ الباحثون عن ميت رومني أخباراً عن المرشَّح الجمهوري للرئاسة في عمليات بحث لاحقة.

قالت غوغل إن التفاوت حدث ببساطة نتيجة الصيغة الرياضية التي اعتمدتها للتوقع باستفهامات المستخدمين. واعتبر تقنيّو غوغل أن جهودهم تساعدنا على اكتشاف ما يطابق حاجاتنا قبل أن نعرف بوجود هذه الحاجات لدينا. ولكن تجدر الإشارة إلى أن الأمر يُعتبر انحيازاً وتدخلاً إذا قامت صحيفة بالأمر نفسه - أُدرجت أخبار أوباما ضمن مقالات عن

معجون أسنان تهمّ بعض القرّاء. وبطريقة مماثلة، تُعتبر الصحيفة منحازة ومتدخلة إذا وضعت إعلانات خاصة بغير الاسوياء جنسياً فقط في صفحات المشتركين الذين تعتبرهم غير أسوياء جنسيين، أو دعايات عن معالجة داء السكّري في صفحات المنتسبين الذين تعتقد أنهم مصابون بالداء.

هل تحصّن التكنولوجيا غوغل من أمر ما لا يكون مقبولاً على الصعيد الاجتماعي في ظروف مختلفة؟ أم أن مارتين أبرامز، وهو خبير رائد في ميدان الخصوصية، مُحِقّ في دعوة هذا النوع من السلوك حالة مقيَّدة حيث "تكون رؤيتي لما هو ممكن محدودة بالحالة" الذي وُضعت فيها؟

يمكن التلاعب بكم مالياً

تملك الشركات التي تجمع مزيداً من البيانات الرقمية عن زبائن محتمَلين القدرةَ على استخدام تلك المعلومات لطلب أسعار مختلفة من مستخدمين مختلفين، أو توجيه مستخدمين مختلفين نحو عروض مختلفة.

يدعو راين كالو، وهو أستاذ قانون في جامعة واشنطن، هذا الأمر إنتاجاً للانحياز بالجملة حيث تستخدم شركاتٌ بياناتٍ شخصية بهدف استغلال عدم مناعة الناس. على سبيل المثال، يمكن للشركات إضعاف قوة إرادة المستهلكين كي يتخلّوا في نهاية المطاف عن القيام بعملية شراء؛ ويمكن لخوارزمية كمبيوترية تحديد السعر لكل فرد يكون مستعداً أو تكون مستعدة لدفعه لقاء مُنتَج أو خدمة ما.

لقد شرعت شركات بطاقات الائتمان باستخدام بعض هذه التقنيات. ففي العام 2010، اكتشفتُ وزملائي في وول ستريت جورنال أن كابيتال وان عرضت بطاقات ائتمان مختلفة (بأسعار مختلفة) لزائري موقعها المختلفين بالاستناد إلى تقديرات عن دخلهم وموقعهم الجغرافي. كانت النتيجة أنه عندما زار توماس بيرني، وهو متعهد بناء من كولورادو، موقع كابيتال وان ، استُقبل بعروضِ بطاقة كابيتال وان بلاتينوم برستيج الخاصة بمن يتمتعون بقدرة كبيرة على الاستدانة. وعندما زارت كاري إسحق، وهي والدة شابة من كولورادو سبرينغ، الموقع، عُرضت عليها بطاقة وُصفت بأنها خاصة بمن يتمتعون بقدرة معتدلة على الاستدانة.

كان السبب مدسوساً في شيفرة الكمبيوتر. ففي الأسطر الـ3,748 من الشيفرة التي تمّ تبادلها بين جهاز كومبيوتر توماس وموقع كابيتال وان تقديراتُ الشركة الخاصة ببطاقة الائتمان عن مستوى دخله (الطبقة الوسطى)، مستواه العِلمي (خرّيج كلّية)، ومدينته (آفون). قدّرت كابيتال وان أن لكاري دخلاً متوسطاً مع دراسة لبعض الوقت في الكلّية . وقال لنا

ناطق بلسان كابيتال وان، "على غرار كل مسوّق، نضع تقييماً بارعاً عبر شبكة الإنترنت وخارجها عما قد يحبه المستهلكون برأينا، وهم أحرار باختيار أي مُنتَج آخر".

في العام 2012، عندما اختبر فريقي مرة أخرى المناورات التجارية في السوق، كانت التقنيات قد أصبحت أكثر انتشاراً وتطوّراً بشكل متزايد. ووجدنا أن شركات بطاقات الائتمان ما تزال تعرض بطاقات مختلفة لمستخدمين مختلفين. كان لدى ديسكوفر عرضٌ هامّ لبطاقة it الخاصة بأجهزة الكمبيوتر التي تُجري اتصالات من مدن مثل دِنفر، كانساس، ودالاس، وليست خاصة بمن يُجرون اتصالات من سكرانتون، بنسيلفانيا؛ كينغسبورت، تينيسي؛ ولوس أنجلوس.

ولكننا وجدنا أيضاً أن أسعار المواقع تتفاوت بالاستناد إلى تقديراتها حول أماكن وجود المستخدمين. في اختباراتنا، باع موقع لوي (Lowe) برّاداً بسعر 449 دولاراً لمستخدمين في شيكاغو، ولوس أنجلوس، وآشبورن، فرجينيا. ولكن كلفته بلغت 499 دولاراً في سبع مدن أخرى. بصورة مماثلة، عُرضت بَكَرة أسلاك كهربائية بطول 250 قدماً بستة أسعار مختلفة على موقع هوم ديبو (Home Depot) وفقاً لموقع المستخدم: 70,80 دولاراً في أشتابولا، أوهايو؛ 72,45 دولاراً في إيري، بنسيلفانيا؛ 75,98 دولاراً في أوليان، نيويورك؛ و77,87 دولاراً في مونتيسيلو. وقالت لوي وهوم ديبو إن الاختلاف في الأسعار يهدف إلى تلاؤمها على الإنترنت مع المتجر الأقرب.

لقد وجدنا الفوارق الأكثر اتساعاً بين الأسعار على موقع عملاق التجهيزات المكتبية ستايبلز (Staples) الذي يستخدم كما يبدو بيانات عن زائرين كي يخمّن أين يقيمون. ويعرض بعد ذلك أسعاراً مختلفة لمستخدمين مختلفين بالاستناد إلى تقديراته حول مكانهم الجغرافي. والنتيجة النهائية: عندما ولجتْ ترود فريتزل موقع Staples.com من جهاز الكمبيوتر في عملها في بيرجيم، تكساس، رأت رزّازة سوينغلاين معروضة للبيع بسعر 14,29 دولاراً. وعلى بُعد أميال قليلة في بورن، رأت كيم وامبل الرزّازة نفسها معروضة على الموقع نفسه بسعر 15,79 دولاراً. لم يحدَّد الفارق استناداً إلى تكاليف الشحن التي تُحتسب بعد شراء السلعة؛ فالأسعار تعكس كما يبدو تقديرات ستايبلز عن المسافة التي تفصل مكان إقامة المستخدمين عن المتجر المنافس. وأكدت ستايبلز أن الأسعار تتراوح نتيجةً لعدد من العوامل، ولكنها رفضت تقديم مزيد من الإيضاحات.

لا يُعتبر تحديد أسعار مختلفة لمستخدمين مختلفين عملاً غير قانوني

ما دام التحديد غير مرتكز على العِرق أو أية معلومات حساسة أخرى تشكل حالة تمييزية. ولكن عرض أسعار مختلفة لمستخدمين مختلفين قد يؤدي إلى نتائج جائرة غير متعمَّدة. لقد أظهرت اختباراتنا التي أجريناها على موقع ستايبلز أن المناطق حيث الدخل المتوسط أعلى قد تكون مرشَّحة للحصول على أسعار مخفَّضة أكثر من المناطق حيث الدخل أكثر انحفاضاً. "أعتقد أنه أمر تمييزيّ جداً"، قالت كيم.

إن أسوأ أنواع المناورات المالية تستغلّ الفقير، المُسنّ، أو الأمّي. تأمّلوا بقوائم المشترين المحتمَلين التي يضعها وسطاء البيانات وتحتوي على أشخاص مُسنّين، في ضائقة مالية، أو غير منيعين بطريقة أو بأخرى في مواجهة بعض أنواع الكلام التسويقي المُقنع. غالباً ما تُباع قوائم المشترين المحتمَلين لمسوّقين مجرَّدين من المبادئ الخلقية يسوّقون لمنتجات احتيالية بكلامهم المنمَّق.

في تشرين الأول/أكتوبر 2012، غرّمت لجنة التجارة الفيدرالية أحد أكبر وسطاء البيانات في البلد، إكويفاكس، وزبائنَه مبلغَ 1,6 مليون دولار بسبب إساءة استعمال بيانات شخصية من خلال بيع قوائم بأشخاص تأخروا على دفع فواتير رهوناتهم الأحدث عهداً لمسوّقين احتياليين. كانت القوائم مسوَّقة بأسماء مثل أَنقذوني من الاستيلاء على الرهن و ندم على الاستدانة . وأحد المشترين مؤسسة سيئة السُّمعة في كاليفورنيا الجنوبية تبيع منتجاتها عبر الهاتف مباشَرةً وحصلت، كما يُزعم، على أكثر من 2,3 مليون دولار من خمسة آلاف مالك منـزل على الأقل دفعوا أقساطاً تتراوح ما بين 1,000 و5,000 دولار بعد تعديلات أُدخلت على القروض دون حدوث هذه التعديلات أبداً. في النهاية، فقد العديد من هؤلاء المالكين منازلهم.

عندما سألتُ موظفة في مؤسسة التسويق المباشَر عما إذا كانت هناك أية قوائم لا يبيعها أفرادها، مثل المُسنّون المصابون بداء الزهايمر الذين يحبون سباق الخيل، أرسلت لي التوجيهات الأخلاقية للمؤسسة التي تحظّر بيع قوائم تحقيرية. ويُسمَح لهم ببيع كل القوائم الأخرى كما يبدو.

يمكن وضعكم في صف لتمييز الوجوه في مركز للشرطة

في 5 نيسان/أبريل 2011، حصل جون غلاس على بريده في نيدهام، ماساشوستس، وتفاجأ لدى عثوره على رسالة تُفيد بإلغاء رُخصة سَوقه. "لقد تفاجأتُ"، قال جون.

فجون عامل في المجلس البلدي - يصلّح سخّانات لمدينة نيدهام. ولا يمكنه القيام بعمله بدون رخصة سَوق. لقد اتصل بمكتب تسجيل المركبات

الآلية في ماساشوستس، وطُلب منه الحضور إلى جلسة استماع وإحضار ما يُثبت هويّته. لم يُطلعوه على سبب إلغاء رخصة سَوقه.

عندما حضر جون إلى جلسة الاستماع، علم بأن مكتب تسجيل المركبات الآلية شرع باستخدام برنامج لتمييز الوجوه بهدف البحث عن عمليات احتيال تطال الهويّة. يقارن البرنامج صور الرخصة لمعرفة الأشخاص الذين يمكن أن يكونوا قد تقدّموا بطلب للحصول على رخص عديدة بأسماء مستعارة مختلفة. لقد أشار البرنامج إلى وجود صور مماثلة له ولشخص آخر يدعى إدوارد بيري من ريهوبوث، ماساشوستس، وطُلب منهما إثبات هويّتهما.

كان جون ضحية ما أدعوه طابور لتمييز الوجوه في مركز للشرطة؛ وهي شبكات تعقُّب تسمح للشرطة بمعاملة الجميع كما لو أنهم مشتبَه بهم. يقلب هذا الأمر نظرتنا التقليدية إلى كيفية تعاطي نظامنا القانوني معنا على أساس أننا أبرياء حتى يَثبت ذنْبنا .

وماسحات الأجساد في المطار هي خير مثال على ذلك. فالماسحات تفتش بالطريقة الأكثر تطفّلاً - تسمح للناظر بإلقاء نظرة متفحصة تحت ملابس المرء - دون وجود أي ارتياب بأن الشخص الممسوح مجرم. في الواقع، يتحمل الفرد الممسوح عبء إثبات براءته أو براءتها، من خلال المرور عبر الماسح الذي قد يُظهر عدم وجود أية أغراض مُريبة. يمكن لشبكات التعقُّب هذه أن تكون كافكيّة. تأمّلوا بقائمة مركز مراقبة الإرهابيين. لا يتم إبلاغ الأشخاص المدرَجين على القائمة بكيفية وصولهم إلى القائمة، ولا يمكنهم مناقشة القرار.

لحسن الحظ، مُنح جون غلاس فرصة الدفاع عن قضيته التي بدت منافية للعقل. لقد عُرضت عليه صورة له تعود لثلاثة عشر عام مضى.

"هي لا تشبهك"، قالت الموظفة.

"بالطبع لا"، قال جون. "مرّ على التقاطها ثلاثة عشر عام. كنت أخفّ وزناً بمئة باوند".

قدّم جون جواز سفره وشهادة المولد، وأُعيدت رخصته إلى وضعها السابق. ولكن الموظفين لم يُعطوه أية ورقة مكتبية تُثبت إعادتها إلى وضعها السابق. أراد الحصول على ورقة ليُثبت لرب عمله أن باستطاعته القيادة ثانيةً. "كان الأمر أشبه بحُلم مزعج"، قال جون.

مستاءً من المعاملة التي تلقّاها وفقدان دخله، تقدّم جون بدعوى قضائية ضد مكتب تسجيل المركبات الآلية، مدّعياً أنه أُنكر عليه حقه

بالإجراءات الرسمية التي يحميها الدستور. جادل المكتب، قائلاً إن جون مُنح فرصة لمناقشة عملية الإلغاء لأن الرسالة وُجّهت بتاريخ 24 أذار/مارس ولم تُلغَ الرخصة حتى أول نيسان/أبريل. لم يتفحّص جون محتويات بريده حتى 5 نيسان/إبريل.

منحت المحكمة العليا لمقاطعة سوفولك مكتب تسجيل المركبات الآلية حق الرفض. واستأنف غاس، ولكن قرار محكمة الاستئناف لم يكن لصالحه أيضاً. "بالرغم من إمكانية فهم امتعاض غاس من اضطراره للدفاع عن هويّته، لا تطرح قضيّته مسائل قانونية أوسع تُلزم محاكم الاستئناف بإيجاد حل لها في هذا الوقت"، قالت المحكمة.

شعر جون بالغدر في العملية برمّتها. هو يتجنّب الآن شرطة الولاية بسبب قلقه من عدم معاملته بإنصاف. "لا نتحكم بقراراتنا كلّياً"، قال. "الأشخاص الطبيعيون وحدهم يرتكبون أخطاء، ولكن لا مجال للسَّهو أبداً".

"أعتقد بالفعل أننا نقايض حرّياتنا بأمننا"، قال.

á á á

توضح هذه القصص حقيقة بسيطة: المعلومات نفوذ. كل من يملك قَدْراً كبيراً من المعلومات يمارس علينا نفوذاً.

في بادئ الأمر، وعد عصر المعلومات بتعزيز قدرة الأفراد على ولوج معلومات كانت مخبَّأة من قَبل وبتمكينهم من المقارنة بين متاجر العالم بحثاً عن أفضل سعر، وأفضل معلومة، وعن الأشخاص الذين يشاطروننا وجهات نظرنا.

ولكن ميزان القوى يتغيّر الآن وتهيمن المؤسسات الكبيرة - المؤسسات الحكومية والشركات - على حروب المعلومات من خلال تعقُّب مقادير كبيرة من المعلومات تتناول المظاهر الرتيبة لحياتنا.

ونُدرك الآن أن باستطاعة الأشخاص الذين يملكون بياناتنا تعريضنا للإحراج، أو إفراغ محفظات نقودنا، أو اتهامنا باتّباع سلوك إجرامي. يمكن لهذه المعرفة بدَورها التسبب بثقافة خوف.

تأمّلوا بشارون وبلال. عندما علما بأنهما مراقبان على PatientLikeMe ، عكفا عن استخدام الإنترنت.

لقد ألغى بلال بريده في المنتدى، وفكك السجل التاريخي لجرعات الدواء الذي كان قد نقله إلى الموقع، وخزّنه في ملف إكسيل على جهازه الكمبيوتري. وكفّت شارون عن استخدام الإنترنت أيضاً ولا تسمح لابنها باستخدامه بدون إشراف.

وشرعا بالتحدث عبر الهاتف، ولكنهما افتقدا الاتصالات التي أجروها عبر PatientLikeMe . "لم أعثر على بديل"، قالت شارون. ووافقها بلال الرأي: "مستخدمو PatientLikeMe يعرفون حقاً كيف يبدو الأمر".

ولكن أيّاً منهما لم يكن قادراً على تحمّل الخوف من الرَّقابة. قالت شارون إنها لم تستطع العيش مع "عدم معرفة ما إذا كان كل ضغط على أحد مفاتيح لوحة الإدخال يسجَّل لدى شركة أخرى". وأضاف بلال، "أشعر فحسب بأن الثقة تراجعت".

تُذكّرنا خبرة شارون وبلال بأن مجد العصر الرقمي كان على الدوام إنسانياً بعُمق بالرغم من كل استعراضاته التكنولوجية. تسمح لنا التكنولوجيا بالعثور على أشخاص يشاطروننا أفكارنا الباطنية، وبإدراك أننا لسنا بمفردنا. ولكن التكنولوجيا تسمح للآخرين أيضاً بالتجسس علينا، حاملةً إيّانا على التراجع عن الإلفة الرقمية.

عندما يسألني الناس عن سبب اهتمامي بالخصوصية، أعود على الدوام إلى الفكرة البسيطة المتمثلة برغبتي في وجود مساحات آمنة خاصة في العالم لأجل شارون وبلال، ولأجلي، ولأجل أبنائي، ولأجل الجميع. أريد أن تكون هناك مساحة في العالم الرقمي لرسائل مُحكَمة الإغلاق بشمع ساخن. هل يجب علينا أن نوجّه على الدوام رسائل على بطاقات بريدية يمكن لأي شخص قراءتها على طول الطريق؟

هل نريد العيش في عالم نكون معرَّضين فيه على الدوام لتسلّلٍ إلى ملفاتنا الكمبيوترية؟ عالم حيث يمكن العثور علينا على الدوام، ولا يمكننا الاحتفاظ بأسرار، ويمكن مراقبتنا حتى في منازلنا، ويمكن انتحال شخصيّتنا، ويمكننا الوقوع في شرَك جدار مرايا ، ويمكن التلاعب بنا مالياً ووضعنا في طابور لتمييز الوجوه في مركز للشرطة؟ هذا الكتاب هو محاولتي للإجابة عن ذلك السؤال في جزأين.

في الفصول الافتتاحية، أستطلع سبب أهمية الرَّقابة غير المميِّزة. للقيام بذلك، أتفحّص الأصول القانونية والتقنية لدولتنا، دولةِ شبكات التعقُّب، واستخدامات الرَّقابة وإساءات استعمالاتها، وتأثيرها على الأفراد والمجتمع.

في الفصول اللاحقة، أتفحّص ما إذا كان هناك أي أمل بإنشاء عالم بديل حيث يمكننا الاستمتاع بثمار التكنولوجيا بدون خوف من أن يتم التسلل إلى ملفاتنا الكمبيوترية. وأختبر استراتيجيات متنوّعة لتجنّب شبكات التعقُّب بدءاً باستخدام هاتف محمول يُدفع رصيد مكالماته مُسبَقاً ويُستبدل تكراراً لإزالة أي أثر لمستخدمه، وصولاً إلى إنشاء هويّات زائفة.

آمل في أن يساعد استطلاعي تطوّرَ الحديث عن الخصوصية وتخطّي مجرّد القلق وسؤال "من يراقبني؟" إلى نقاش ذات درجات اختلاف أكثر دقة وسؤال "ما أهمية ذلك؟" وفي النهاية، التوصل إلى حديث مُنتِج عما يمكننا القيام به في هذا الشأن.

الفصل الثاني

موجَز تاريخ التسلل إلى الملفات الكمبيوترية

بعد سبعة أسابيع من الهجمات الإرهابية التي قتلت آلاف الأشخاص ودمّرت مركز التجارة العالمي في نيويورك، خرج للمرة الأخيرة أحد أبرز الأشخاص الذين يحلّون الشيفرة في البلد من وكالة التجسس الأهم في الولايات المتحدة.

حدث ذلك في 31 تشرين الأول/أكتوبر 2001. كانت مانهاتن السفلى ما تزال تحترق ويتصاعد منها الدخان. لقد وُجّهت رسائل تحتوي على جَمرة خبيثة إلى أعضاء في الكونغرس ووسائل إعلام في مختلف أنحاء البلد، وكان يتمّ الإبلاغ كل يوم، كما يبدو، عن حالات رُعب بسبب شائعات عن وجود قنابل. كان بلداً قلقاً في حرب مع عدوّ خفيّ.

ولكن بيل بيني، وهو شخص يحلّ شيفرة كان قد بلغ مستوى عميد في وكالة الأمن القومي، لم ينضمّ إلى المعركة. لقد تقاعد بعد أكثر من ثلاثين عاماً قضاها في الوكالة. عندما بلغ أسفل السلّم في مقرّ قيادة الوكالة في فورت ميد، ماريلاند، قال، "أصبحت حرّاً أخيراً. أصبحت حرّاً أخيراً".

قضى بيني سنوات في محاولة عصرنة وسائل رَقابة وكالة التجسس وتمكينها من مراقبة الاتصالات عبر شبكة الإنترنت الناشطة في مختلف أنحاء العالم، محترماً في الوقت نفسه خصوصية اتصالات المواطنين الأميركيين. ولكنه كان يرى جهوده تُحبَط مع كل منعطف.

وعندما أخبره زملاؤه بأن الوكالة تجمع اتصالات المواطنين الأميركيين دون أن يأخذوا بعين الاعتبار الحماية التي تتمتع بها الخصوصية، لم يشأ المشارَكة في ذلك.

أثناء مغادرة مجمَّع فورت ميد، كان بيني يهرب مما اعتبره مسرح جريمة. "لم أتمكن من البقاء بعد شروع وكالة الأمن القومي بانتهاك الدستور عن عَمد"، أعلن في وقت لاحق في شهادة في المحكمة ضد مستخدِمه السابق.

كنا نعرف مذاك الحين، بالطبع، أن بيني مُحِق. فبعد هجمات 11/9 الإرهابية، أنشأت الحكومة الأميركية شبكات تعقُّب واسعة النطاق، غير قانونية على الأرجح، تضع يدها على حركة الاتصالات الهاتفية والبريد الإلكتروني لكل أميركي تقريباً.

á á á

أثناء بحثي لفهم تاريخ وأصول الرَّقابة الجماعية، كنت أعود باستمرار إلى العام 2001. لم يكن عامَ الهجمات الإرهابية المدمِّرة فحسب في الولايات المتحدة، بل العام الذي تُركت فيه صناعة التكنولوجيا مصابةً بالدُّوار بسبب جيشان تقنية الـ com المنبجس. وأطلق هذان الحدثان غير المرتبطَين في الظاهر سلسلة أحداث أدّت إلى الدعامات القانونية والتقنية لشبكات التعقُّب الحالية. بالنسبة إلى الحكومة الأميركية، أظهرت الهجمات الإرهابية أن الوسائل التقليدية لجمع المعلومات الاستخباراتية لم تكن ناجحة. وبالنسبة إلى سيليكون فالي، أظهر الانهيار المالي الحاجةَ للعثور على وسيلة جديدة لجَني المال.

لقد توصّل الجانبان إلى الحلّ عينه لمشاكلهما المتباينة: جمع كميات ضخمة من البيانات الشخصية، وتحليلها.

بالطبع، لكل منهما غاية مختلفة. كانت الحكومة تسعى إلى العثور على إرهابيين قد يكونون مختبئين وسط الشعب، واقتلاعهم، وتسعى صناعة التكنولوجيا إلى إغواء معلِنين يملكون ملفات متينة عن الأفراد. ولكن الفريقَين أصبحا متشابكَين، وهو أمر حتميّ، بسبب استخدام الحكومة الأميركية نفوذها للغوص في بيانات صناعة التكنولوجيا.

معاً، أنتجت الحكومة وصناعة التكنولوجيا دولة شبكات التعقُّب. في ما يلي كيف بدأ كل شيء.

á á á

في القرن الثامن عشر، كان البريطانيون يمرون في وقت عصيب أثناء مراقبة مستعمراتهم الأميركية، ويثور الأميركيون ضد المحاولات البريطانية لمنع التجارة بين المستعمرات ودول أوروبية أخرى، وضد المطالب البريطانية بدفع ضرائب دون الحصول على تمثيل في البرلمان.

ولمواجهة وباء التهريب، أنشأ البريطانيون نوعاً جديداً من تقنية الرَّقابة: مذكَّرات تفتيش عامة تُعرف بالمذكرات القضائية وتسمح للضباط البريطانيين بالقيام بما يعادل بحثاً بعيداً عن الشُّبهات من منـزل إلى منـزل.

كان الأميركيون غاضبين بسبب تمكن الضباط البريطانيين من اقتحام أي منـزل في أي وقت، حتى أثناء زفاف أو جنازة. "يبدو لي أسوأ وسيلة لممارسة النفوذ بطريقة تعسّفية"، ناقش المحامي جايمس أوتيس الابن في خُطبة شهيرة في بوسطن عام 1761.

ساعدت حالة الغضب من مذكرات التفتيش العامة على قيام الثورة

الأميركية. والغضب من مذكرات التفتيش العامة هي أساس التعديل الرابع في الدستور الأميركي، ويقول: " لا يجوز المساس بحق الناس في أن يكونوا آمنين بأشخاصهم ومنازلهم ومستنداتهم ومقتنياتهم من أي تفتيش أو احتجاز غير معقول، ولا يجوز إصدار مذكرة بهذا الخصوص إلا في حال وجود سبب معقول معزَّزٍ باليمين أو التوكيد، وتُبيّن بالتحديد المكان المراد تفتيشه والأشخاص أو الأشياء المراد احتجازها".

فالتعديل الرابع هو مبدأٌ أساس لموظفي إنفاذ القانون في الولايات المتحدة. ولكن التكنولوجيا مكّنت من استغلال مكامن الغموض القائمة في تفسير التعديل الرابع. في ما يلي بعض نقاط الغموض الأكثر أهمية:

- **المساحة العامة** . يحمي التعديل الرابع "الأشخاص، المنازل، المستندات، والأوراق". لقد فسّرت المحكمة العليا هذا الأسلوب الإنشائي بحيث يعني أنه لا يمكن للأفراد أن يتوقعوا التمتع بالخصوصية علَناً. ولكن التكنولوجيا قلّصت الحدود الحمائية للمساحة الخاصة من خلال التمكين من مراقبة استعمال الكمبيوتر في المنازل، ومن خلال طائرات بدون طيار تحلّق فوق الفناءات.
- **مبدأ الطرف الثالث** . أنشأت المحكمة العليا مبدأ الطرف الثالث الذي ينص على أنه لا يمكن للأفراد أن يتوقعوا تمتُّع المعلومات التي يمنحونها لطرف ثالث بالخصوصية؛ كمصرفهم أو شركة هاتفهم. نتيجةً لذلك، يمكن الحصول في غالب الأحيان على معلومات حساسة مخزَّنة لدى طرف ثالث، كالبريد الإلكتروني مثلاً، دون مذكرة تفتيش.
- **ما وراء البيانات** . ما وراء البيانات تعني بيانات عن البيانات - على سبيل المثال، إن المغلف الذي يحتوي على رسالة يمكن اعتباره ما وراء البيانات، والبيانات هي الرسالة بذاتها. لقد وضعت المحكمة تقليدياً معايير قانونية تبسيطية للبحث عن ما وراء البيانات . على سبيل المثال، يستطيع مركز البريد التقاط صورة فوتوغرافية لمغلّف رسالتكم بدون مذكرة تفتيش، ولكنه لا يستطيع فتح الرسالة بدون مذكرة تفتيش. في العصر الرقمي، يمكن لما وراء البيانات أن تكشف عن كثير من الأمور، ككل أرقام الهاتف التي تتصلون عليها، والأشخاص الذين توجهون لهم رسائل بريد إلكتروني، ومكان إقامتكم.
- **عمليات بحث حدودية** . دعمت المحاكم على نطاق واسع استثناء عمليات البحث الحدودية من التعديل الرابع، ويسمح الاستثناء للحكومة بالقيام بعمليات بحث على الحدود دون الحصول على مذكرة

تفتيش. في العصر الإلكتروني الحالي، يعني ذلك أن باستطاعة العملاء نقل المحتويات الكاملة لهاتف أو جهاز كمبيوترٍ فردٍ على الحدود - غالباً ما يقومون بذلك. تقول الجمارك ودوريات حرس الحدود الأميركية إنها تُجري نحو خمس عشرة عملية بحث إلكترونية في اليوم. وفي أذار/مارس 2013، وضعت محكمة الاستئناف للدائرة التاسعة في كاليفورنيا حداً جديداً لإخضاع الأجهزة على الحدود لعمليات بحث، وذلك بعد إصدارها حكماً في قضية الولايات المتحدة ضد كوترمان مفاده أن الشُّبهة المنطقية بوجود نشاط جنائي تتطلب إخضاع الجهاز لعملية بحث جنائية - كاستخدام برنامج أو تحليل بيانات مشفَّرة أو مُلغاة، وهي الحالة المرادفة لإلقاء نظرة على عجَل على مستندات، صور فوتوغرافية، أو ملفات أخرى.

في العصر الرقمي، أصبحت مكامن الغموض هذه كبيرة بما يكفي للسماح بإجراء عمليات بحث بعيدة عن الشُّبهة تُغضب الآباء المؤسسين.

á á á

لقد حرص الرؤساء الأميركيون على الدوام على عدم تجاوز حدود التعديل الرابع.

ففي العام 1981، عندما أجاز الرئيس رونالد ريغان القيام بعمليات تجسس محلية محدودة بحثاً عن متسللين سوفيات، أمر وكالات الاستخبارات باعتماد "مجموعة التقنيات الأقل تطفّلاً التي يكون استخدامها ملائماً داخل الولايات المتحدة، أو الموجَّهة ضد أشخاص أميركيين في الخارج". على مَرّ السنين، فُسِّر توجيه ريغان كي يعني أنه يُفترض ممارسة عمليات التجسس المحلية بحذر وفي حالات وجود سبب للاشتباه بجريمة.

ولكن بعد 11/9، وُضعت جانباً، وبحكم الواقع، الحاجة إلى وجود شُبهة من نوع ما قبل خوض حروب تجسس محلية. وترسم المستندات التي كشف عنها المتعاقد السابق مع وكالة الأمن القومي، إدوارد سنودن، صورة مدمِّرة عن كيفية قيام قرار واحد اتُّخذ في الأيام التالية للهجوم بفتح بوّابات ضبط التدفّق في شبكات التعقُّب المحلية. ووفقاً لمسوَّدةِ تقريرٍ مسرَّبة وضعها المفتش العام عام 2009، شرعت وكالة الأمن القومي بالتجسس المحلي في 14 أيلول/سبتمبر 2001، أي بعد ثلاثة أيام من الهجمات، عندما وافق مدير الوكالة، مايكل هايدن، على اعتراض أي اتصال هاتفي، وبدون مذكرة تفتيش، يُجرى من الولايات المتحدة بأرقام هاتفية محدَّدة في أفغانستان تُعتبر إرهابية، أو يتمّ تلقّيه في الولايات المتحدة من أرقام هاتفية من أفغانستان تُعتبر إرهابية. وفي 26 أيلول/سبتمبر، وسّع

هايدن الأمر ليغطّي كل أرقام الهاتف في أفغانستان.

ولكن سرعان ما أراد هايدن مزيداً من البيانات. كان على ثقة بوجود فجوة دولية بين ما تجمعه وكالة الأمن القومي في الخارج وما تبحث عنه الأف بـي آي في الداخل. لم يكن أحد يراقب الاتصالات الواردة إلى الولايات المتحدة من الخارج. لذلك، عمل هايدن مع نائب الرئيس، ديك تشيني، الذي طلب من مستشاره القانوني المساعدة على وضع مسوَّدة مذكّرة قانونية تساعد وكالة الأمن القومي على ملء الفجوة الدولية. وفي 4 تشرين الأول/أكتوبر، أصدر الرئيس جورج دبليو بوش مذكّرة بعنوان، "إجازة رَقابة إلكترونية معيَّنة للنشاطات في فترة محدَّدة لاكتشاف ومنع أعمال إرهابية داخل الولايات المتحدة". سمحت المذكرة لهايدن بمواصلة استهداف الاتصالات بين أفغانستان والولايات المتحدة دون طلب موافقة محكمة الرَّقابة الاستخباراتية الخارجية التي تشرف في العادة على الرَّقابة الإلكترونية التي تطال السكان الأميركيين. وأُجيز البرنامج لمدة ثلاثين يوماً.

في ذلك الوقت، بدا الأمر أشبه بإجراء اضطراري يمكن فهمه. ففي عصر يشهد تمكّن الإرهابيين من إخفاء حركة اتصالاتهم عبر الإنترنت من خلال إرسالها إلى مختلف أنحاء العالم، كان من الصعب أحياناً التمييز بين الاتصالات الأميركية والاتصالات الخارجية. لقد منح الأمر وكالة الأمن القومي راحة مؤقّتة من عملية فرز الاتصالات الأميركية في زمن الأزمات.

من جهة ثانية، أعدّ هايدن بعناية برنامجاً قصير الأمد تَحوّل في النهاية إلى جهد تجسّسي محلّي مكتمل النموّ. لقد جُدّد الأمر الذي يدوم ثلاثين يوماً إلى ما لا نهاية، ووُسِّع. في غضون عام، توسّع ليشمل اتصالات أميركية - دولية وليس الاتصالات الأميركية - الأفغانية فقط. واستخدمت وكالة الأمن القومي الأمر الرئاسي لتبرير الحصول على البريد إلكتروني والاتصالات الهاتفية لآلاف الأهداف في آن. وبدأت أيضاً بتلقّي مقدار كبير من سجلات الاتصالات الدولية والبعيدة المدى، وذلك بهدف إجراء عملية ربط ، أي العثور على شخص اتصل بشخص آخر قام بالاتصال بإرهابيّ مشتبَه به. وبدأت وكالة الأمن القومي بجمع حركة الاتصالات عبر الإنترنت (من ترسلون لهم بريداً إلكترونياً وصفحات الويب التي تزورونها) من مصادر تجمع غالبية الاتصالات من مصادر أجنبية ويكون هناك احتمال كبير لجمع حركة اتصالات إرهابية.

لجمع هذه البيانات، سعت وكالة الأمن القومي إلى تعاون مع شركات الإنترنت والهواتف. ويشير التقرير إلى الاتصال بسبع شركات (لم تُذكر

أسماؤها) رفضت ثلاث منها المشاركة.

في العام 2005، كشفت نيويورك تايمز عن قصة برنامج التنصت دون الحاجة إلى مذكرات تفتيش، واصفةً إيّاه بنقلة كبرى في ممارسات جمع المعلومات الاستخباراتية. واتضحت عملية جرف البيانات التي يقوم بها البرنامج على نطاق واسع بعد أشهر قليلة عندما أعلن تقنيّ متقاعد في أيه تي أند تي، مارك كلين، خبر قيام وكالة الأمن القومي بتثبيت تجهيزات في غرفة سرّية عائدة لمكتب أيه تي أند تي في سان فرانسيسكو يمكنها التنصت على كل الاتصالات المتدفقة عبر ذلك الجزء من الإنترنت. "هذه هي البنية التحتية لدولة بوليسية أورويلية. يجب إغلاقها!" قال كلين في بيان علَني.

بعد ذلك، نشرت يو أس أيه توداي في أيار/مايو 2006 مقالة جاء فيها أن أيه تي أند تي، فِريزون، وبِلساوث، شرعت بتزويد وكالة الأمن القومي بسجلات الاتصالات الهاتفية الخاصة بزبائنهم بعد فترة وجيزة من 11/9. "إنها قاعدة البيانات الأكبر التي جُمعت يوماً في العالم"، قال مسؤول مجهول الاسم استُشهد به في المقالة.

تحت الضغط، أغلق الرئيس بوش أجزاء من البرنامج لمدة وجيزة. ولكنه أضاف توقيعه في العام 2008 على التعديلات القانونية التي أُدخلت على قانون الرَّقابة الاستخباراتية الخارجية، مما أعاد برنامج التنصت إلى وضعه السابق وجعله قانونياً، وحصّن موفّري الاتصالات ضد الدعاوى القضائية التي يمكن أن تُرفع عليهم بسبب مساهمتهم السابقة في برنامج غير قانوني ربما.

لقد أرست التعديلات التي أُدخلت على قانون الرَّقابة الاستخباراتية الخارجية نوعاً جديداً من مذكرات التفتيش تسمح للحكومة باعتراض اتصالات دون الحصول على اسم المستهدَف - مواصلةً بشكل أساسي عمليات الجرف الواسعة التي قامت بها من خلال التنصت دون الحاجة إلى مذكرات تفتيش. ولكن في هذه المرة، تعيّن حصول الخوارزمية المعتمَدة لاستهداف المشتبَه بهم على موافقة قاضٍ. لقد وصف برنامج بريسم، الذي كشف عنه سنودن، شركات الإنترنت المُذعنة لمذكرات التفتيش التي تطال الخوارزميات. وكافحت ياهو!، كما يبدو، لإعلان إحدى مذكرات التفتيش غير دستورية في جلسة استماع سرّية في المحكمة، ولكنها خسرت الدعوى وأُجبرت على الإذعان لمذكرات التفتيش تحت تهديد اتهامها بالازدراء المدَني.

وتبيّن أن التنصت دون الحصول على مذكرة تفتيش كان أحد برامج

وكالة الأمن القومي التي خضعت لمزيد من الضبط لأنها تعترض فقط الاتصالات الصادرة من الولايات المتحدة إلى بلدان أجنبية، وهو أمر مثير للدهشة. وتعرّضت المقادير الكبيرة للاتصالات عبر الهاتف والإنترنت، التي شرعت وكالة الأمن القومي بجمعها داخل الولايات المتحدة، لمزيد من الجرف. وبما أنها بيانات عن بيانات، جادلت وكالة الأمن القومي، قائلةً إن جرف سجلات الاتصالات الهاتفية وحركة الاتصالات عبر الإنترنت لا ينتهك الخصوصية الأميركية.

لقد كشف سنودن عن أمر سرّي صادر عن المحكمة يُلزِم فِريزون بتسليم سجلات الاتصالات الهاتفية اليومية لوكالة الأمن القومي. بعد فترة وجيزة، أكدت السيناتور ديان فينشتاين عن ولاية كاليفورنيا قيام وكالة الأمن القومي بجمع سجلات اتصالات هاتفية محلية ودولية من كل شركات الاتصالات الكبرى طوال سبع سنوات.

وكشف سنودن أيضاً عن مذكرة تعود للعام 2007 وضعها محامٍ في وزارة العدل، يدعى كينيث وينشتاين، حثّ فيها على منح وكالة الأمن القومي سلطة قانونية لجمع مزيد من الاتصالات عبر الإنترنت داخل الولايات المتحدة. "من خلال استخدام الخوارزميات الكمبيوترية، توجِد وكالة الأمن القومي سلسلة اتصالات تربط الأشخاص الموصِلين للمعلومات"، كتب وينشتاين. "يتعيّن إيقاف الممارسة الحالية لوكالة الأمن القومي عندما تصطدم سلسلة ما برقم هاتف أو عنوان يُعتقد أنه مستخدَم من قِبل شخص أميركي". ومن ثم، طلب الإذن من النائب العام لإجراء "عملية ربط للاتصالات" التي يُجريها السكان الأميركيون.

لقد تمّت الموافقة على رغبته لمدة وجيزة، كما يبدو. وقالت إدارة أوباما إن برنامج مراقبة حركة الاتصالات عبر الإنترنت انتهى عام 2011 ولم يُشرَع فيه من جديد. ولكن ما تزال وكالة الأمن القومي تراقب، على الأرجح، حركة الاتصالات المحلية عبر الإنترنت تحت ستار آخر.

بصرف النظر عن ذلك، أكدت الأمور التي كشف عنها سنودن ما كان محطَّ شُبهة لدى العديدين: نمت شبكة تعقُّب صغيرة لمدة ثلاثين يوماً، تغطّي الاتصالات الأميركية - الأفغانية، لتصبح شبكة تعقُّب محلية كبيرة.

á á á

بعد 11/9، دعم اندفاعٌ كبير للإنفاق على مكافحة الإرهاب رَقابةً من خلال شبكات التعقُّب المحلية وعلى مستوى الولايات. فارتفعت ميزانيات وكالة الاستخبارات الفيدرالية من 27 بليون دولار قبل الهجمات إلى 75

بليون دولار عام 2013. ورشح بعض تلك الميزانية إلى الولايات على صورة هِبات.

تأملوا بنشاطات وزارة الأمن الداخلي ليس إلا. فمنذ 11/9، وزّعت الوزارة أكثر من 7 بليون دولار من الهِبات لمساعدة المناطق المدينية ذات كثافة سكانية عالية والمعرَّضة لتهديد كبير بهدف تجنّب الإرهاب والرد عليه. ووُزّع أكثر من 50 مليون دولار من هِبات وزارة الأمن الداخلي على وكالات إنفاذ القانون لشراء قارئات لوحات تسجيل مؤتمَتة تمكّنهم من مراقبة تحركات المواطنين بطرق لم تكن ممكنة من قَبل. وساعدت الوزارة أيضاً على تمويل إنشاء "مراكز صهر" في كل ولاية تقريباً تتولى مهمة سحق بيانات من وكالات مختلفة - ومن وسطاء بيانات تجارية في غالب الأحيان - بهدف البحث عن إلماعات تمكّنها من تجنّب أعمال إرهابية في المستقبل. وشرعت الشرطة المحلية بشكل متزايد بتعقُّب الناس، مستخدمين إشارات تبثّها هواتفهم المحمولة.

في الوقت نفسه، أصبحت التحقيقات البعيدة عن أية شُبهة أكثر شيوعاً. ففي العام 2008، أصدر النائب العام توجيهات جديدة تسمح للأف بـي آي بإطلاق تحقيقات بدون "أي تأكيد دقيق مستنِد إلى وقائع". وفقاً للقواعد الجديدة، أُسندت إلى الأف بـي آي مهمة الحصول على معلومات ذات منفعة استقصائية ممكنة عن أفراد، مجموعات، أو منظمات، إما بسبب احتمال تورّطهم في نشاطات جنائية أو مهدِّدة للأمن القومي، أم بسبب احتمال كونهم مستهدَفين بهجمات أم ضحية هذه النشاطات".

وفي العام 2012، أجازت وزارة العدل لـالمركز القومي الأميركي لمكافحة الإرهاب نَسخ قواعد بيانات حكومية كاملة عن مواطنين أميركيين - سجلات الرحلات الجوية، قوائم بموظفي الكازينو، أسماء الأميركيين الذين يستضيفون طلاباً أجانب وفقاً لمبدأ تبادل الطلاب - وتفحّص الملفات بحثاً عن أي سلوك مثير للرِّيبة.

في السابق، كان يحظَّر على الوكالة تخزين معلومات عن السكان الأميركيين ما لم يكن الشخص مشتبَهاً به بارتكاب أعمال إرهابية أم أنه على صلة بتحقيق ما.

أصبحت شبكات التعقُّب البعيدة عن أية شُبهة المقياس الجديد.

á á á

بشّرت هجمات 2001 الإرهابية أيضاً بعصر شبكات التعقُّب في سيليكون فالي.

حتى أواخر التسعينات، كانت صناعة البرامج الكمبيوترية الاستهلاكية مجرد تجارة بالمفرّق، فتباع البرامج في عُلب ملفوفة بمادة انكماشية على رفوف المتاجر. بالطبع، كانت الشركات تشتري أيضاً برامج صناعية بالجملة. ولكن السوق الشعبي - المكوَّن في الغالب من ألعاب وأدوات للإنتاجية المكتبية - كان يعتمد التجارة بالمفرّق.

لقد أطاح الإنترنت بتجارة البرامج الكمبيوترية كلّياً.

فأول جزء حقيقي من برنامج كمبيوتري على الإنترنت هو متصفِّح نتسكيب نافيغايتر على الويب الذي أُنتج عام 1994. وبات نتسكيب سلعة جماهيرية أوّلية مرتفعة الثمن بسبب توقُّع ظهور أول برنامج كمبيوتري يحظى بأوسع مجموعة من المستهلكين. لقد ارتفع سعر سهم الشركة المنتجة في أول يوم من طرحه في الأسواق المالية، مُنهياً اليوم بأربعة أضعاف سعر طرحه الأساسي. ووجد المؤسس المشارك لنتسكيب، مارك أندريسن، والبالغ من العمر أربعاً وعشرين عاماً فقط، نفسه مع ثروة تقدَّر بـ171 مليون دولار. في العام التالي، وُضعت صورة أندريسن على غلاف مجلة تايم حافياً وعلى رأسه تاج، وإلى جانب صورته دون التعليق التالي: المهرجون الناجحون.

ولكن الأرباح لم تُحقَّق أبداً. لقد شرعت مايكروسوفت بتضمين نظام تشغيلها ويندوز 95 متصفّحاً مجانياً على الويب يدعى إنترنت إكسبلورر. نتيجةً لذلك، لم تتمكن نتسكيب أبداً من فرض رسوم على برنامجها الكمبيوتري.

عام 1998، قاضت وزارة العدل ونواب عامّون من عشرين ولاية، إضافةً إلى مقاطعة كولومبيا، مايكروسوفت، زاعمين أنها تصرفت بطريقة احتكارية بربط إنترنت إكسبلورر بـويندوز 95. ولكن مع توقيع مايكروسوفت مرسوم الموافقة عام 2002، أُحدث الضرر. في العام 1998، تفوّق إنترنت إكسبلورر على نتسكيب في سوق الأسهم، وفي العام 2008 جرى التخلي عن برنامج نتسكيب رسمياً.

لقد أُنتج أول برنامج جماهيري حقاً، ولكنه لم يحقق أية أرباح. كانت العِبرة واضحة: انتهى سوق البرامج الكمبيوترية بالمفرّق. ولكن التكنولوجيا تتطلب برامج. كيف تمّ التمويل؟

بادئ ذي بدء، بدا الأمر كما لو أن الإعلان قد يكون الجواب. ففي أواخر التسعينات، كانت سيليكون فالي مغمورة بالمؤسسات التي تعتمد تقنية الـ com ، وقد استند العديد منها على فرضية قيام الإعلان بدعم جهودها. ولكن الجيشان انبجس عام 2000. ورأت ياهو!، التي تجني مداخيلها في

الغالب من الإعلان عبر شبكة الإنترنت، انخفاض رسملتها السوقية من 113,9 بليون دولار في أوائل عام 2000 إلى 7,9 بليون دولار فقط بعد عام.

أصبحت الحكمةُ التقليدية إخفاقَ الإعلان عبر الإنترنت. "منذ عامَين، كان كل المعلنين تقريباً يقولون، يجب أن أكون على الإنترنت"، قال بات ماكغراث، المدير التنفيذي الأول في وكالة أرنولد ماكغراث الإعلانية، في تشرين الثاني/نـزفمبر 2001. "اليوم، يخطون إلى الوراء قائلين، هل من المنطقي اعتبار الإنترنت إحدى الوسائل الترويجية لهذا النوع من السِّلع؟" وتردد صدى تخمين ماكغراث عبر صناعة الإنترنت. كانت ويندي تايلور، محررة زيف دايفيس سمارت بيزنيس، الأكثر إيجازاً وبلاغة. "خمد الإعلان عبر الإنترنت"، أعلنت.

واتُّهمت صناعة لديها أفضل الأدوات لقياس حجم جمهورها في تاريخ الإعلان بعدم امتلاك أية وحدات قياس لإثبات فعالية مُنتَجها. وبدأت شركات الإنترنت بالبحث عن معايير قياسية أفضل. باستطاعة تكنولوجيا تعقُّب عظيمة، تتمثل بقيام موقع على الويب بإرسال قَدْر قليل من البيانات وتخزينها في متصفّح المستخدم، تتبُّع مستخدمي الويب من موقع إلى موقع. ولكن لم يتّضح مدى قانونيّتها.

في العام 2000، رُفعت دعوى قضائية فيدرالية جماعية ضد شركة الإعلان على الإنترنت، دابل كليك، مدّعيةً أن قيامها بإنـزال تكنولوجيا التعقُّب الآنفة الذِّكر على أجهزة كمبيوتر زائري مواقع الويب ينتهك القوانين التي تحدّ من التنصّت، والتسلل إلى الملفات الكمبيوترية، والرقابة الإلكترونية. بعد عام، حكمت القاضية نعومي رايس بوخفالت، في المقاطعة الجنوبية لنيويورك، بأن أعمال دابل كليك غير قانونية لأن مواقع الويب أجازت لـدابل كليك إنـزال تكنولوجيا التعقُّب الآنفة الذِّكر على أجهزة كمبيوتر زائريها. "نجد أن مواقع الويب المُلحَقة بـدابل كليك مشارِكة بمعلومات المدَّعين الذين منحوا موافقتهم الكافية لـدابل كليك كي تعترضها"، كتبت. لقد بلغ حكمها حد منح مواقع الويب حرّية الرَّقابة: عندما يزور شخص ما موقعاً على الويب، يكون الموقع حرّاً بدعوة آخرين للتنصّت على الزائر بشكل سرّي.

أخيراً، بات لسيليكون فالي نموذج للأعمال: التعقُّب.

á á á

بالطبع، طالما قامت الشركات الخاصة بجمع بيانات عن زبائنها وموظفيها. ولكن شراء البيانات الشخصية وبيعها لم يصبح صناعة حتى ظهور

أداء كمبيوتري معاصر.

في العام 1971، طلب رب عمل فينود غوبتا منه الحصول على قائمة بكل تاجر للمنازل النقّالة في البلد. فجلس غوبتا، وهو مهاجر حديث العهد من الهند حائز على شهادة ماجستير في إدارة الأعمال من جامعة نيبراسكا، مع مجموعة من أدلّة المِهن والشركات، وشرع بابتكار قائمته الخاصة. وسرعان ما أدرك أنه لا بد من وجود طريقة أفضل لوضع قائمة تسويقية. في العام 1972، أسس شركة تدعى أميريكان بيزنيس إينفورمايشن استخدمت جداول الصفحات الصفراء لوضع قوائم عن الزبائن تكون بتصرّف المسوِّقين. وسرعان ما شرعت الشركة، المعروفة الآن بإينفوغروب، بعمل جديد متمثل بتضمين القوائم بيانات من الصفحات البيضاء، وشرعت بشراء بيانات من اتحادات مِهنية وغَرْف أي نوع من البيانات العامة المتوافرة - من سجلات رُخص السَّوق، إلى بطاقات تسجيل الناخبين، إلى سجلات المحاكم.

"كل قائمة متوافرة تقريباً"، قال غوبتا لاحقاً. "إذا كنتم تريدون لاعبي غولف أعسَرين، أو صيّادي أسماك أعسَرين، أو صيّادي أسماك يستعملون حشرات طبيعية أو اصطناعية، أو مالكي كلاب، فكل تلك القوائم متوافرة".

في الجانب المقابل من البلد، في كونواي، أركنساس، كانت شركة أخرى تواجه المشكلة نفسها. ففي العام 1969، أسس تشارلز وارد، وهو رجل أعمال محلّي ناشط في الحزب الديموقراطي، شركة صغيرة تدعى ديموغرافيكس إينك. لمساعدة المرشَّحين المحليين على إدارة حملات مباشَرة عبر البريد. لقد ساعدت شركته دايل بامبرز في حملته الانتخابية لمنصب حاكم أركنساس، ولويد بِنتسِن في محاولته الفاشلة لبلوغ سدّة الرئاسة، قبل أن تتوسّع في النهاية إلى ما وراء الميدان السياسي. في العام 1989، بدّلت الشركة اسمها إلى أكسيوم.

حلّقت أكسيوم في التسعينات بسبب حاجة الأعمال إلى شركات تمتلك خبرة كمبيوترية لإدارة بيانات زبائنها. وبين عامَي 1993 و1998، تضاعفت مداخيل أكسيوم أربع مرات من 91 مليون دولار إلى 402 مليون دولار. "كانت البيانات هناك على الدوام"، قال دونالد هينمان، وكان مديراً تنفيذياً في أكسيوم آنذاك، لـ واشنطن بوست عام 1998. "يمكنكم ولوجها الآن فقط بواسطة التكنولوجيا".

لقد دعمت مجموعات البيانات الجديدة النفيسة الشركات الجديدة. ووجدت شركتا بطاقات الائتمان كابيتال وان وديسكوفر طرقاً لتقطيع السكان إلى شرائح ومكعَّبات صغيرة مفيدة يمكن استهدافها من خلال البريد المباشَر.

وأصبح بيع البيانات عملاً مُربِحاً للحكومات على كل المستويات. فولاية فلوريدا وحدها تكسب نحو 62 مليون دولار في العام من بيانات رُخَص السَّوق. وتحقق الخدمة البريدية في الولايات المتحدة دخلاً سنوياً يبلغ 9,5 مليون دولار، ممكّنةً شركات مثل أكسيوم ولوج قاعدة بيانات التغيير الوطني للعناوين.

في العقد الأول من القرن الحادي والعشرين، ومع انتشار الإنترنت، ظهر اهتمام المسوِّقين بالبيانات الأحدث عهداً المتعلقة بمواقع الويب التي يتصفحّها الناس. كان القرار القانوني الصادر بحق دابل كليك قد ولّد صناعة كاملة مكرَّسة لتتبُّع كل نقرة على الإنترنت يقوم بها مستخدمو الويب. وفي العام 2007، انضمّ كل عمالقة الإنترنت إلى عملية التعقُّب عبر الإنترنت. لقد اشترت أيه أو أل شركة تاكودا، التي تعتمد طريقة الاستهداف السلوكي لزيادة فعالية حملتها على شبكة الويب، بملغ 275 مليون دولار، ودفعت غوغل 3,1 بليون دولار لـدابل كليك، ودفعت مايكروسوفت 6 بليون دولار للشركة الإعلانية عبر الإنترنت أيه كوانتيف. كانت كل تلك الشركات تضع سِيَراً شخصية ومِهنية عن مستخدمي الويب.

كان رد فعل وسطاء البيانات سريعاً. فشرعت أكسيوم، مع آخرين، بالعمل على دمج ملفاتها مع سجلات تصفّح الويب، ممكّنةً المعلنين من استهداف إعلانات على الإنترنت بدقة استهداف بريدهم. في الوقت نفسه، شرعت أكسيوم ببيع بياناتها لشركات مثل فيسبوك التي أرادت تعزيز عملية تعقّبها.

ودعَم التعقُّب عبر الإنترنت صناعة جديدة أيضاً: الاتجار بالبيانات. ففي البورصات المماثلة لسوق الأوراق المالية، يشتري المُعلنون ويبيعون نُبذات عن الزبائن في عمليات تجارية تجري في كل جزء من ألف ثانية. يجري الأمر على النحو التالي: عندما تبحثون عن كاميرا رقمية في إي باي (eBay)، تكون صفحة الويب مرفَقة بشيفرة خاصة بشركةٍ لتبادل البيانات مثل بلوكاي. عندما تُنبِّه بلوكاي إلى وجودك على الصفحة، تبيع على الفور الرسائل الموجَّهة من الجهاز الخادم إلى متصفّح الويب لمعلنين يريدون الوصول إلى مشتري الكاميرا. ويفوز المساوم الأفضل بحق تزويدك بإعلان عن كاميرا رقمية في الصفحات التالية التي تزورها. لهذا السبب، يبدو الأمر كما لو أن إعلانات الإنترنت تلاحقك في غالب الأحيان أينما تذهب.

ينمو الإعلان عبر الإنترنت بسرعة، ويعود سبب ذلك، إلى حد كبير، إلى تقنية التعقُّب. لقد ارتفعت مداخيل الصناعة من 7,3 بليون دولار فقط

عام 2003 إلى 36,6 بليون دولار عام 2012. فالتعقُّب بالغ الأهمية بالنسبة إلى الصناعة لدرجة قول راندال روثنبرغ، رئيس إنتراكتيف أدفرتايزينغ بيرو، "إن بلايين الدولارات التي يجنيها الإعلان عبر الإنترنت، ومئات آلاف الدولارات التي تجنيها المؤسسات المعتمدة على الإعلان عبر الإنترنت، ستختفي" إذا فقدت الصناعة قدرتها على تعقُّب الناس.

أوجزت ميجلينا كونيفا، عضو اللجنة الأوروبية، الأمر بشكل أفضل عام 2009 عندما قالت: "البيانات الشخصية هي النفط الجديد للإنترنت والنَّقد الجديد للعالم الرقمي".

á á á

إذا أردتم وضع تصنيف للمتعقّبين، فهو سيبدو مماثلاً لما يلي:

الحكومة

- **جامعون عرَضيون.** الوكالات التي تجمع بيانات أثناء مسار عملها الطبيعي، مثل مكاتب الولايات لتسجيل المركبات الآلية ودائرة الإيرادات الداخلية، ولكنها غير منخرطة مباشَرةً في تجارة البيانات.
- **محقِّقون.** وكالات تجمع بيانات عن مشتبَه بهم كجزء من تحقيقات لإنفاذ القانون، مثل الأف بـي آي والشرطة المحلية.
- **محلّلو بيانات.** نوع جديد من الوكالات التي تغرف بيانات من وكالات حكومية ووسطاء بيانات تجارية، وتحلّلها، كالمراكز التي يزوّدها مجهودٌ جماعي لعدة وكالات بموارد وخبرة ومعلومات (Fusion center)، والمركز القومي الأميركي لمكافحة الإرهاب.
- **جاسوسية.** وكالات كوكالة الأمن القومي يُفترض بها التركيز على التجسس الخارجي، ولكنها حوّلت اهتمامها إلى التجسس المحلي أيضاً.

عمل تجاري

- **جامعون عرَضيون.** هم في الأساس كل المؤسسات التي تجمع معلومات شخصية في سياق عملها المنتظم، وتتراوح بين مؤسسات التنظيف على الناشف المحلية، والمصارف، وموفّري وسائل الاتصالات.
- **متبارون بأسلوب حر.** شركات البرامج الكمبيوترية في الغالب، مثل غوغل وفيسبوك، التي توفّر خدمات مجانيّة وتجني مالاً من بيانات زبائنها - من خلال بيع المسوِّقين حق ولوج البيانات.
- **مسوِّقون.** إن نشوء التعقُّب عبر الإنترنت كأساس للعمل الإعلاني التجاري وضع المسوِّقين بشكل أساسي في ميدان تجارة البيانات.
- **وسطاء البيانات.** شركات تشتري من جامعي بيانات حكوميين

وتجاريين عرَضيين، وتحلّل البيانات، وتُعيد بيعها. ويبيع البعض، مثل أكسيوم، البيانات لمؤسسات بشكل أساسي. وتبيع شركات أخرى، مثل إنتليوس (Intelius)، لأفراد بشكل أساسي.

- **بورصة البيانات.** يتّجر المسوّقون ووسطاء البيانات باطّراد بمعلومات في مكاتب تَداول فورية تحاكي سوق الأوراق المالية.

أفراد

- **شبكات تعقُّب جُعلت ديموقراطية.** أصبحت التكنولوجيا رخيصة بما يكفي لدرجة تمكّن الجميع من القيام بتعقباتهم بواسطة أدوات مثل كاميرا لوحة القيادة، وطائرات بدون طيار تجمعونها بأنفسكم، ونظّارات غوغل غلاس التي تحتوي على كاميرات بالغة الصِّغر باستطاعتها التقاط صور وأفلام فيديو.

المتعقّبون متشابكون إلى حد كبير. والبيانات الحكومية هي قِوام الحياة لوسطاء البيانات التجارية. وتعوّل شبكات التعقُّب الحكومية على الحصول على معلومات من القطاع الخاص.

تأمّلوا مَثل واحد فقط: الاقتراع. للتسجّل بهدف الاقتراع، يجب على المواطنين ملء استمارة حكومية تتطلب في العادة الاسم والعنوان، وفي حالة واحدة تقريباً، تاريخ المولد. ولكن قلّة من الناخبين يُدركون أن تلك القوائم تُباع في غالب الأحيان لوسطاء بيانات تجارية. لقد وجدت دراسة جرت عام 2011 أن قائمةً للناخبين على مستوى الولايات بيعت بـ30 دولاراً، كحد أدنى، في كاليفورنيا وبـ6,050 دولاراً كحد أقصى، في جورجيا.

يدمج وسطاءُ البيانات التجارية المعلومات الاقتراعية مع بيانات أخرى لوضع نُبذات غنيّة بالمعلومات عن أفراد. على سبيل المثال، يسوّق وسيط البيانات أرسطو إينك. قدرته على تمييز 190 مليون ناخب بواسطة أكثر من 500 معلومة عن المستهلكين مستندة إلى وقائع كالتصنيف الائتماني وحجم رهنهم.

واحزروا من يشتري بيانات شركة أرسطو المخصَّبة؟ سياسيون يستخدمون أحياناً مالاً حكومياً. وتتباهى الشركة بأن "كل رئيس أميركي - ديموقراطي وجمهوري - من ريغان إلى أوباما، استخدم منتجات الشركة و/أو خدماتها". في الواقع، وجدت أطروحة مِقدامة تعود للعام 2012، وضعتها طالبة جامعة هارفارد، ميليسا أوبنهايم، أن واحداً وخمسين عضواً من مجلس النواب

الأميركي اشتروا بيانات من شركة أرسطو، مستخدمين بعض العلاوات الممنوحة للكونغرس، مما سمح لهم بجمع معلومات عن ناخبيهم الذين هم في سنّ أبنائهم، وما إذا كانوا مشتركين بمجلات دينية أم يملكون رخصة صيد. وهكذا، تقع البيانات في إطار ما تدعوه أوبنهايم "دورة البيانات العملانية غير المستخدَمة". وتحتاج الحكومة إلى قيام مدنيين بجمع بيانات تبيعها بعد ذلك إلى كيانات تجارية تقوم بتبييض البيانات وإعادة بيعها للحكومة.

تحدث دورة البيانات العملانية غير المستخدَمة مع كل نوع من البيانات تقريباً. فسجلات المركبات الآلية على مستوى الولايات مجروفة إلى داخل تقارير لكسيس نكسيس، وتعزَّز ببيانات أخرى وتُباع لوزارة الأمن الداخلي. وتعالَج سجلات الحجز في محاكم على مستوى الولايات، وتُجمَع بعد ذلك من قِبل وسطاء بيانات مثل كورلوجيك التي تبيع رِزم بياناتٍ عقارية لزبائن بمن فيهم الحكومة.

وتجري دورة بيانات عملانية غير مستخدَمة في محكمة الرَّقابة الاستخباراتية الخارجية حيث يمكن للحكومة أن تطلب من الصناعة الخاصة تسليم بيانات عن زبائنهم. في ظل تلك الظروف، أُرغمت شركات عملاقة مثل غوغل، ياهو!، فِريزون، ومايكروسوفت، على تسليم بيانات عن الزبائن لوكالة الأمن القومي.

á á á

لقد عانى بيل بيني بسبب التكلم جَهاراً ضد شبكات تعقُّب وكالة الأمن القومي.

فأثناء وجوده في الوكالة، طوّر بيني ما اعتقد أنه شبكة تعقُّب تحترم الخصوصية الفردية وتحميها. فالبرنامج المدعوّ ثين ثريد ذكيّ ويعترض مقادير كبيرة من البيانات المرسَلة عبر الإنترنت والهاتف، يشفّرها، ويحلّلها على صورة أنماط. لا يمكن فك شيفرتها إلا في حال وجود تهديد محدَّد وموافقة المحكمة على إصدار مذكرةِ تفتيشٍ لفك شيفرة البيانات.

ولكنه لم يتمكن من نشر البرنامج. وبعد عدة سنوات من المعارك الداخلية، وأثناء قيام بيني وزملاؤه بنقل قضيّتهم إلى قادة في الكونغرس مباشَرةً، رفض القادة الأعلى مرتبة في وكالة الأمن القومي دعم ثين ثريد. أحد الأسباب: في مرحلة ما قبل 11/9، كان محامو الوكالة قلقين من انتهاك ثين ثريد خصوصية الأميركيين بسبب قدرته على جمع اتصالات محليّة بالرغم من كونها مشفَّرة. وهناك سبب آخر: دعم مدير الوكالة، مايكل هايدن، برنامجاً أكثر كلفة يدعى ترايل بلايزر وضعه متعاقدون خاصّون

ويهدف إلى تحليل مقادير عظيمة من بيانات وكالة الأمن القومي، ولكنه لا يستخدم التشفير. تمّ التخلّي عن ترايل بلايزر في نهاية المطاف بعد تجاوز الكلفة الضخمة وإخفاقات تقنية.

في العام 2002، اتصل زميل بيني، كيرك إيبـي الذي عمل على ثين ثريد، بالمفتش العام في وزارة الدفاع كي يُبلغه بما يعتقد أنه "هَدر، احتيال، وإساءة استعمال" في وكالة الأمن القومي. لقد نُقِّح تقرير المفتش العام، الذي صدر عام 2005، إلى حد كبير، ولكن الأجزاء القليلة غير المنقَّحة بدت أنها تبرّئ ثين ثريد.

عام 2006، نشرت بالتيمور صن مقالة عن المعارك الجارية حول ثين ثريد. "وكالة الأمن القومي رفضت النظام الذي غربل البيانات الهاتفية بشكل قانوني"، جاء في العنوان الرئيسي.

وفي 26 تموز/يوليو من العام 2007، أغارت الأف بـي آي على منـزل بيني في ضواحي ماريلاند.

كان بيني في الحمّام. "دخل الرجل وصوّب مسدساً نحوي". تذكّر. "فقلت، هل تفترض أن باستطاعتي ارتداء بعض الملابس؟"

لقد أُغير أيضاً في هذا اليوم على إيبـي، الذي كان قد تقاعد من وكالة الأمن القومي في يوم تقاعُد بيني. لم يُتّهم أيّ من بيني أو إيبـي بأية جريمة أبداً.

في 28 تشرين الثاني/نوفمبر 2007، أغارت الأف بـي آي على منـزل مؤيّد آخر لـثين ثريد، توماس دريك، وهو مدير تنفيذي في وكالة الأمن القومي تعاون أثناء التحقيق الذي أجراه المفتش العام دون الإشارة إلى اسمه. استولى العملاء على أوراق دريك، وأجهزته الكمبيوترية، وأقراص صلبة، وزعموا أنهم عثروا على مستندات سرّية في الطابق السفلي. بعد عامَين ونصف، أُدين دريك وأُتُّهم بانتهاك قانون التجسس بسبب "احتفاظه المتعمَّد" بمستندات سرّية.

لقد دُمِّر دريك مالياً بسبب المقاضاة. كان ما يزال يتبقّى لديه خمسة أعوام ونصف للتقاعد من الوكالة. ففقد راتبه التقاعدي البالغ 60,000 دولار في العام. وحصل على رهنٍ ثانٍ لقاء منـزله وسحب معظم مدخراته التقاعدية وفقاً لمخطط 401 (كيه) لتسديد نفقاته. لم يكن بالإمكان توظيفه في ميدان الاستخبارات، لذلك شرع بالعمل في متجر لأبل يبيع بالمفرَّق. بعد إنفاق 82,000 دولار على رسوم قانونية، أعلنته المحكمة مُعدَماً وقام بتمثيله محامٍ عام.

عام 2011، وبعد موجة إعلانية عن محنة دريك، أسقطت الحكومة التُّهم الجنائية العشر الموجَّهة لدريك، شريطة اعتراف دريك بذَنْبه في "تجاوز الاستخدام المسموح به لجهاز كمبيوتر حكومي". أثناء إصدار الحكم، وصف قاضي المحكمة الجزئية الأميركية، ريتشارد دي. بينيت، فترةَ التأخير البالغة عامَين ونصف بين البحث وتوجيه التُّهَم بأنها "لا أخلاقية". إنه أحد الأمور الأكثر أهمية في وثيقة الحقوق المتمثل بعدم قيام هذا البلد بتعريض الناس للخطر من خلال القرع على أبوابهم بدعم من الحكومة ودخول منازلهم"، كتب. "وعندما يحدث هذا الأمر، يجب القيام به بسرعة كبيرة".

لم يَتهم القاضي بينيت الحكومةَ صراحةً باستخدام النفوذ لإزعاج مسرِّبِ معلوماتٍ سرّية. ولكنه أصدر بحق دريك أدنى حكم ممكن - مراقَبة لمدة عام، وُطلب منه أثناء ذلك خدمة المجتمع لمدة شهر، ولا غرامات مالية. وأغلق جلسة المحاكمة مخاطباً دريك: "أتمنّى لك أفضل الحظ في بقية حياتك".

قبل مقاضاة دريك، حاول بيني، دريك، وإيبـي، إصلاح الوكالة من الداخل. ولكن مع دنوّ محاكمة دريك، أعلنوا عن الأمر. وبعد تبرئة دريك، كرّسوا كل وقتهم لانتقاد وكالة الأمن القومي، مُجرين مقابلات لاذعة مع وسائل الإعلام، ومحذّرين من نفوذ وكالة غير مدقَّق بنشاطاتها تملك معلومات عن الجميع.

عندما التقيت بيني للمرة الأولى، استهل كلامه، قائلاً إن كمية البيانات التي جمعتها وكالة الأمن القومي تفوق بعشرات المرات كمية البيانات المتوافرة لدى الشرطة السرّية الأكثر قمعاً في العالم ألا وهي الغستابو، والشتازي، والـكيه جي بـي.

"إنه لَخطر حقيقي عندما تجمع حكومةٌ ذلك القدر من المعلومات عن المواطنين"، قال لي. "إن جمع ذلك القدر من المعلومات يمكّنهم من التحكم بالجميع".

الفصل الثالث
دولة رَقابة

الرَّقابة ليست نشاطاً مريعاً بحد ذاتها.

فالأهل يراقبون أبناءهم للحرص على عدم إلحاق الأذى بأنفسهم. وضباط الشرطة يراقبون السكان لإلقاء القبض على المجرمين. والشركات تراقب موظفيها للإمساك باللصوص والغشاشين. والصحافيون يراقبون مؤسسات متمتعة بالنفوذ للكشف عن إساءات استعمال.

ولكن عصر شبكات التعقُّب الحديث يسجّل نوعاً جديداً من الرَّقابة: بعيدة عن الشُّبهة، تجري من خلال أجهزة الكمبيوتر، موضوعية، وواسعة النطاق. يعتقد بعض الأشخاص أن هذه الرَّقابة ستوفر مزيداً من الأمن للمجتمع، ويعتقد آخرون أنها تبشّر بدولة بوليسية.

لفهم السيناريو الأسوأ لهذه الحالة، زرتُ المحفوظات التي تلقى أفضل عناية في العالم وتعود إلى ما قبل الرَّقابة الإلكترونية - محفوظات الشتازي في برلين. أردت رؤية كيفية احتفاظ الشتازي، وهي الشرطة السرّية الألمانية الشرقية في الحقبة الشيوعية، بالملفات، مقارَنةً مع المعلومات التي تجمعها عمليات الرَّقابة التجارية والحكومية في الوقت الحاضر.

كانت الشتازي الشرطة السرّية الأكبر في تاريخ العالم - مقارَنةً بعدد السكان. ذائعة الصيت بممارستها للقمع، احتفظت الشتازي بملفات 4 ملايين ألماني شرقي - أو نحو ربع مجموع السكان البالغ 16,7 مليون نسمة. لم تكن التكنولوجيا الحالية متوافرة للشتازي - تعيّن عليهم فتح البريد والإصغاء إلى الاتصالات الهاتفية يدوياً - ولكن كان لديها شبكة واسعة من المُخبرين. في العام 1989، كان ألمانياً شرقياً واحداً من كل خمسين ألمانياً شرقياً، بين سنّ الثامنة عشرة والثمانين، يعملون لصالح الشتازي بطاقة معيَّنة.

مع انهيار النظام الألماني الشرقي في تشرين الثاني/نوفمبر 1989، شرع الشتازي بتدمير الملفات التي احتفظ بها عن المواطنين. غاضبين من إتلاف الدليل على ظلم النظام، اقتحم المواطنون مقر قيادة الشتازي لإيقاف عملية إتلاف الملفات. نتيجةً لذلك، يمكن للمواطنين في الوقت الحاضر أن يطلبوا رؤية الملفات التي تمّ الاحتفاظ بها عنهم، ويمكن للباحثين ولوج بعض الملفات، ولكن أسماء الأشخاص المراقَبين أُزيلت.

في رحلة إلى برلين عام 2011، توقفتُ في مركز محفوظات الشتازي -

المعروف رسمياً بالمفوضية الاتحادية للحفاظ على سجلات جهاز أمن الدولة في جمهورية ألمانيا الديموقراطية السابقة - الواقع بشكل غير مناسب في مبنى مكاتب برّاق ذي نوافذ زجاجية في قلب المدينة.

أبدا مدير سجلات الشتازي، غونتر بورمان، حماسةً فورية لفكرتي المتمثلة بمقارنة رَقابة الشتازي مع الرَّقابة الحديثة. وأثناء ملئي الورقة الكتابية للحصول على مجموعة سجلات الشتازي، سألني عما يعرف جامع بيانات غربـي نموذجي عني. لذلك، سألتُ عما إذا كان بإمكاني استخدام جهازه الكمبيوتري لأُريه القليل مما يُعرف عني على شبكة الإنترنت.

فدخلتُ حسابـي على بريد غوغل الإلكتروني وأبحرتُ إلى الإعدادات حيث سمح لي غوغل برؤية أبحاثي السابقة على الويب، بما في ذلك الكتب التي بحثتُ عنها والصور التي رأيتها، إضافةً إلى قائمة الأشخاص الثلاثة والتسعين الذين كنت قد وجّهت لهم رسائل عبر البريد الإلكتروني، أم وجّهت لهم رسائل فورية عبر بريد غوغل الإلكتروني.

واقفاً فوقي، ترك هذا الأمر انطباعاً قوياً في نفسه. "كانت عملية تنظيم شبكة اجتماعية"، قال لي، "أمراً شديد الصعوبة بالنسبة إلى الشتازي". وجلس إلى طاولة المؤتمرات وشرع برسم دوائر قليلة بواسطة خطوط متصلة. "حاولوا تنظيم شبكة اجتماعية"، قال، ولكنهم واجهوا صعوبة كبيرة في وضع خرائط متينة بالرغم من عدد المُخبرين لديهم.

مُلهَمة، دخلت صفحتي على LinkedIn - حيث أعددت برنامجاً خاصاً يُستخدم كجزء من متصفِّح الويب (Plug-in) يسمح لي برؤية تصوّرٍ عن شبكتي الاجتماعية. كانت خارطة جميلة مع نحو مئتَي نقطة موصولة ببعضها بخطوط ملوّنة، وكل زملاء العمل في نيويورك مجمَّعون في زاوية صفراء، وزملاء آخرون في وسائل الإعلام مجمَّعون في زاوية زرقاء، واتصالاتي التي أجريتها عندما كنت في كاليفورنيا مجمّعة على الجانب الآخر للخارطة في بحر برتقالي مع نقط رمادية.

لقد أحدث ذلك انطباعاً أكبر في نفس بورمان. "كان الشتازي ليحبون هذا الأمر".

á á á

بعد ثلاثة أشهر، وصلت رِزمة مستندات إلى طاولتي في نيويورك. كان يوجد في داخلها أكثر من مئة صفحة تحتوي على ملفَّين باللغة الألمانية. بعد قليل من البحث، عثرت على بعض خبراء الشتازي لمساعدتي على ترجمة وتفسير الملفَّين.

لقد تفاجأتُ بمدى فظاظة الرَّقابة. "كان البريدُ، والهاتف، وكل المُخبرين، تكنولوجيا الرَّقابة الرئيسية المعتمَدة"، قال غاري بروس، أستاذ تاريخ مُشارِك في جامعة واترلو، ومؤلّف كتاب المؤسسة: قصة المعلومات السرّية للشتازي .

لقد كشف الملف الأول رَقابةً منخفضة المستوى تدعى إيمفورغانغ غايتها تجنيد هدف مجهول الهوية ليصبح مُخبِراً. (أسماء الأهداف منقّحة؛ أسماء عملاء الشتازي غير منقَّحة). في هذه الحالة، كان الشتازي يراقبون طالب مدرسة ثانوية مُمِلّ يُقيم مع والدته وشقيقته في شقة عاديّة. حصل الشتازي على تقرير عنه من مدير مدرسته ومن النادي المنتسب إليه.

لم يكن الشتازي يملك معلومات كثيرة عنه - سبق لي أن رأيت نُبذات تحتوي على مقدار أكبر من المعلومات - ولكنهم واصلوا محاولة تجنيده كمُخبِر. لقد رفض طلبهم، ذاكراً بعض الأسباب الصحية غير المحدَّدة. كان محظوظاً لأنه صغير السنّ ومُمِلّ. ومعظم الناس الذين يُطلب منهم أن يكونوا مُخبِرين يشعرون بأنهم لا يستطيعون ردّ طلب الشتازي عندما يواجَهون بدليل على ارتكابهم مخالفة طفيفة - كمشاهدة المحطة التلفزيونية الألمانية الغربية.

يوثّق الملف الثاني عملية رَقابة تُعرَف بـ OPK ، أي *Operative Personenkontrolle* ، وتستهدف رجلاً كان واضعاً لشعرٍ معارض. إنها عملية متوسطة الحجم: نشر الشتازي ثلاثة مُخبِرين لمراقبته، ولكنهم لم يفتحوا بريده أو يُصغوا إلى اتصالاته الهاتفية.

كان ضباط الشتازي يتلقون مكافآت عندما يُطلقون عمليات رَقابة، لا بل يتلقون أيضاً مكافآت أكثر سخاء إذا كانت العملية مُثمرة - اعتقال أحد الأشخاص أو الفوز بمُخبِر جديد. في النهاية، لم تكن عملية رَقابة الشاعر مُثمرة لأن النظام انهار قبل أن يتمكن الشتازي من اتخاذ أي إجراء ضده.

بعد ستة أشهر، وصلت رِزمة أصغر حجماً، كنت قد طلبتُها، تحتوي على نحو خمس عشرة صفحة توثّق تكتيكات رَقابة محدَّدة تعتمدها الشتازي.

في أحد الملفَّين، سجّل عملاء الشتازي تحركات رجل في الأربعين من العمر لمدة يومَين - 28 و29 أيلول/سبتمبر 1979. لقد راقبوه أثناء إنـزال غسيله، وتحميل سيارته بلفافات ورق جدران، ونقل طفل في سيارة "ملتزماً بحدود السرعة"، متوقفاً لملء سيارته بالوقود، ومسلِّماً ورق الجدران لمبنى سكنيّ. واصل الشتازي تعقُّب السيارة أثناء قيام امرأة بإعادة الطفل إلى

برلين.

"كانت الأهداف شديدة الحذر..."، كتب ضابط الشتازي، المقدَّم فريتش. "لقد حُذّروا مُسبَقاً... كما هو مُفترَض... بأن عمليات مراقبة تجري في الجِوار".

بدأ العميل بتعقُّب الهدف، كما يبدو، عند الساعة 4:15 من مساء يوم جمعة. وعند الساعة 9:38 مساءً، دخل الهدف شقته وأضاء الأنوار. بقي العميل طوال الليل وسلّم عملية الرَّقابة لعميل آخر عند السابعة من صباح يوم السبت. يبدو أن ذلك العميل تعقّب الهدف حتى الساعة العاشرة صباحاً. من وجهة النظر الحالية، يبدو ذلك عملاً كبيراً لأجل معلومة صغيرة.

كان الملف الثاني شبكة اجتماعية مرسومة باليد. لقد رسم العملاء على صفحة واحدة أربعاً وستين عملية وصل، رابطين الهدف بأشخاص متنوّعين ("عمّة"، "قضية جنتشيك العملياتية"، بيرند جنتشيك كما هو مُفترَض، وهي شاعرة ألمانية شرقية انشقّت ولجأت إلى الغرب عام 1976)، أماكن ("كنائس")، ولقاءات ("عبر البريد، عبر الهاتف، لقاء في المجر").

كانت مستنداً مثيراً للاهتمام. فربع بياناته فقط مشابهة لصِلاتي التي تفوق المئتَين على صفحتي على LinkedIn ، ولكنها ذات صلة بالتحقيق، على الأرجح، أكثر منه بشبكتي الواسعة.

قام الشتازي على الأرجح بمهام رَقابة شملت كل من هو موجود على الخارطة، وكانوا يُعرفون بـ"الأفراد الثانويين"، وفقاً لغاري بروس. "ليس عليك القيام بأي شيء مُعارض بصفة خاصة لينتهي بك الأمر ملفاً لدى الشتازي".

لقد تمثلت المشكلة بأن ملف الشتازي - مهما كان كبيراً - يؤثّر في تخفيض رُتبة الشخص، أو ترقيته، أو في مدة انتظاره للحصول على سيارة أو شقة، أو ما إذا كانت ستتم الموافقة أم لا على طلبه زيارة أنسبائه في الغرب. نتيجةً لذلك، وبالرغم من امتلاك الشتازي ملفات لربع السكان فقط، كان الخوف من التحول إلى هدف منتشراً.

في تقرير العام 1990، بعد سقوط النظام الشيوعي مباشَرةً، وصف 72,6 بالمئة من مواطني ألمانيا الشرقية الاختبار الشيوعي بأنه "رَقابة تامة". في العام 1992، وعندما طُلب من الذين طالهم الاستفتاء التفكير مليّاً في البيان التالي، "يشعر المرء بأن هناك من يتجسس عليه. لا يمكنكم الثقة بأحد"، وصفه 43 بالمئة بأنه "صحيح، هذا ما كان عليه الحال بالتحديد".

وفي دراسة تناولت الآثار النفسية لرَقابة الشتازي، أجرت بابيت باور

مقابلة مع نحو ثلاثين شخصاً كانت لهم لقاءات مباشَرة مع الشرطة السرّية. ووجدت أن الخوف من لقاء آخر مع الشتازي حثّهم إما ليصبحوا مواطنين نموذجيين أو لينسحبوا من المجتمع. واستنتجت باور أن الأشخاص الذين التقوا الشتازي كانوا يُخفون كَبتاً داخل "تجاعيد الجسم وآليات الدماغ".

á á á

كان الـبانوبتيكون - تصميمُ سجن اقترحه جيريمي بنثام عام 1787 - الفكرةَ الأساسية لتكون المراقبة قمعية. تتمثل فكرته بأن سجناً مثالياً سيسمح للسجناء بالاعتقاد أنهم مراقَبون طوال الوقت، ولكنه يسمح للمراقبين بالبقاء غير مرئيين. لقد صمّم سجناً دائرياً مع برج حراسة في الوسط، ولكنه لم يُبنَ أبداً في حياته.

في العام 1975، روّج الفيلسوف الفرنسي ميشال فوكو لفكرة بنثام، واصفاً البانوبتيكون بأنه أداة نفوذ "مدهش". "كلما كان أولئك المراقبون مجهولو الهوية والمؤقَّتون أكثر عدداً، ازدادت إمكانية تفاجؤ النـزيل وإدراكُه القلِق بأنه مراقَب"، جاء في كتابه السلوك والعقوبة .

أما ونحن نعيش اليوم في عالم من الرَّقابة الواسعة، فمن المنطقي أن تكون حالتنا الذهنية الجماعية مماثلة لإدراك فوكو القلِق. ولكن فوكو كان مُحِقاً جزئياً فقط، كما يبدو. فكما اكتشفت بابيت باور في مقابلاتها مع ألمانيين شرقيين، يتعاطى الناس مع الرَّقابة بقدر ازدياد قلقهم من تغيير سلوكهم.

عام 2011، ثبّت باحثون فنلنديون تجهيزات مراقبة واسعة - كاميرات فيديو، ميكروفونات، أجهزة كمبيوتر، هواتف ذكية، وأجهزة مراقبة تلفزيونية - لدى عشر عائلات لمدة عام بهدف تحديد أثر الرَّقابة الكلّية الوجود، الطويلة الأمد. لقد وجدوا أن الأشخاص موضع الدراسة - من الواضح أنهم تطوّعوا ـ"اعتادوا الرَّقابة تدريجياً". ومع ذلك، كانت ردود الفعل متباينة. لقد خرج أحد المشاركين من الدراسة بعد ستة أشهر، قائلاً إن الرَّقابة اختصرت استخدامه أو استخدامها للكمبيوتر، وأثّرت في علاقاته أو علاقاتها. (لم يكشف الباحثون عن الجنس أو يحددوا تفاصيل الأشخاص موضع الدراسة).

وبالرغم من معرفة الأشخاص موضع الدراسة أنه لن يتمّ الكشف عن البيانات الناجمة عن الرَّقابة لأي شخص باستثناء الباحثين، وباستطاعتهم إطفاء النظام في أي وقت، فقد وجدوا المراقبة مصدر "إزعاج، وقلَق، وهمّ، لا بل غضب أيضاً"، كتب الباحثون. ووسائل المراقبة المكروهة أكثر من

سواها هي أجهزة الكمبيوتر وكاميرات الفيديو (أقرّ مشاركان أنهما كانا يُطفآنها بانتظام).

وغيّر معظم المشاركين أعمالهم الروتينية، ولا سيما مكان خلع ملابسهم (لم توضَع كاميرات في غرف النوم أو الحمّامات) وحيث يُجرون أحاديث حساسة.

"شرع شخصان ممن كان خاضعين للدراسة بقضاء مزيد من الوقت في غرفة النوم التي لا تغطيها الميكروفونات. وقال آخران إنهما كانا يتوجهان إلى المقهى لمناقشة مسائل شخصية"، كتب المؤلّفون. "وذكر أحد الأشخاص أنه تجنّب دعوة عدة أشخاص إلى منـزله".

قال المؤلف الرئيسي للمقالة، وهو باحث في علم الكمبيوتر يدعى أنتي أولاسفيرتا، إنه بالرغم من استقرار قلق الأشخاص الصريح في شأن الخصوصية بعد ثلاثة أشهر، فقد عدّلوا بأجمعهم سلوكهم للتكيّف مع الوضع. ولكن تكيّفاتهم كُدِّرت بسهولة. "لقد جعلت التغييرات المنـزل هشّاً" وأي حدث اجتماعي غير متوقَّع كان يضع الممارسات الجديدة في الواجهة وتُطرح تساؤلات حولها، ويحول أحياناً دون القيام بهذه الممارسات".

á á á

يصف مؤلّف روايات خيالية، ديفيد برين، في كتابه المتبصّر الصادر عام 1998 المجتمع الشفاف: هل تُرغمنا التكنولوجيا على الاختيار بين الخصوصية والحرّية؟ طريقةً أخرى للتعاطي مع الرَّقابة الكلّية الوجود.

يبدأ الكتاب بـ"قصة مدينتَين". ففي المدينتَين كاميرات للرَّقابة مثبَّتة على "كل عمود مصباح، وكل سطح ولافتة شارع". في المدينة الأولى، تُبثّ كل الصور إلى مركز الشرطة المركزي. في المدينة الثانية، يمكن لكل مواطن ولوج أية كاميرا من خلال تلفاز على صورة ساعة يد.

والمدينتان خاليتان من الجريمة. ولكن المدينة الأولى دولة بوليسية، في حين أن الثانية تتمتع ببعض الحرّية: "يتحقق متمشٍّ في وقت متأخر من المساء من عدم تربّص أحدهم وراء الزاوية... تُنعم والدة قلقة النظر بالمنطقة للتحقق من الطريق التي سلكها طفلها هائماً على وجهه... يُلقى القبض على سارق متاجر باحتراس... لأن الضابط المعتقِل يعرف أن العملية برمّتها تخضع لتفحّص دقيق".

ويناقش برين باقتناع، قائلاً إن انتشار الكاميرات - وتكنولوجيا أخرى للرَّقابة - هي النتيجة الحتمية لتقدّم التكنولوجيا. بالنسبة إليه، إن السؤال الهام هو التالي: من يتحكم بالكاميرات؟ برأيه، يمكن للرَّقابة المتبادَلة -

المواطنون والدولة يراقبون أحدهم الآخر - تحويل الرَّقابة الكلّية الوجود من القمع إلى تحميل مسؤولية متبادلة. وفي ما يلي دليل يدعم وجهة النظر هذه.

أثناء الحرب الباردة، لعبت الرَّقابة المتبادَلة دوراً هاماً في منع الولايات المتحدة والاتحاد السوفياتي من إلقاء قنابل نووية على أحدهما الآخر.

فبعد إطلاق الاتحاد السوفياتي المركبة الفضائية سبوتنيك عام 1957، اعترى أميركا خوف من قدرات الاتحاد السوفياتي ومعانيها الضمنية. في العام 1958، ادّعى السيناتور جون أف. كينيدي أن الولايات المتحدة تتخلّف عن السوفيات، وتنبّأ بأن "الولايات المتحدة ستفقد تفوّقها بحلول العام 1960... كونها قوة نووية ضاربة".

لم تتمكن الولايات المتحدة من قياس مدى تأخرها عن الاتحاد السوفياتي في إنتاج الصواريخ إلا عندما نجحت في إطلاق أقمار تجسس صناعية للاستطلاع عبر التقاط صور فوتوغرافية. وأظهرت الصور الملتقَطة بواسطة القمر الصناعي أن التأخر الحقيقي في الإنتاج سلك اتجاهاً مختلفاً: عام 1961، كان السوفيات يمتلكون أربعة صواريخ بالستية عابرة للقارات، مقارنةً مع مخزون من 170 صاروخاً بالستياً أميركياً عابراً للقارات.

من جهة ثانية، كانت الولايات المتحدة لا تزال غافلة عن التعاظم الصاروخي السوفياتي في كوبا في صيف العام 1962، وهو إخفاق استخباراتي وضع الولايات المتحدة والاتحاد السوفياتي على شفير حرب نووية. نتيجةً لذلك، أصبح إنشاء أقمار تجسس صناعية أفضل جزءاً هاماً من سباق التسلّح في الحرب الباردة.

عام 1972، نظّمت الولايات المتحدة والاتحاد السوفياتي أعمالهما التجسسية في معاهدة الحد من الصواريخ البالستية عندما وافق كل جانب على استخدام "وسائل تقنية وطنية" للتحقق من إذعان الجانب الآخر لبنود المعاهدة. بعد ست سنوات، أقرّ الرئيس جيمي كارتر، في خطاب له في مركز كينيدي للفضاء، بأهمية أقمار التجسس الصناعية. حيث قال: "أصبحت الأقمار الصناعية للاستطلاع عبر التقاط صور فوتوغرافية عاملَ استقرار هام في شؤون العالم المرتبطة بمراقبة اتفاقيات مراقبة التسلّح".

بالفعل، قد تكون الرَّقابة العلنية فعالة في تغيير السلوك البشري. لقد أظهرت الدراسات تكراراً أن الإيحاء البسيط بأن المرء مراقَب يمكن أن يشجع الناس على التصرف بشكل متعاون أكثر - حتى ولو لم تكن هناك رَقابة فعلية.

إن الاعتقاد بوجود شخص آخر يُحدث حالة "استيقاظ نفسيّ" حتى ولو لم يكن ذلك "الشخص" حقيقياً، وفقاً لراين كارلو من جامعة واشنطن. في إحدى الدراسات، تبين أن الأشخاص الذين يحدّقون بصورة روبوت منتفخ العينَين يُضيفون مالاً إلى الصندوق المشترك في لعبة كمبيوترية أكثر بنسبة 30 في المئة من أولئك الذين يشعرون بأنهم غير مراقَبين.

عام 2011، علّق باحثون في جامعة نيوكاسل في بريطانيا، ولمدة اثنَين وثلاثين يوماً، ملصقات كبيرة لعيون بشرية تحدّق على مستوى العين بأماكن عشوائية في كافتيريا حرَم الجامعة. لقد وجدوا أن الأشخاص الذين ينظفون طاولاتهم بعد الانتهاء من تناول الطعام تضاعف، مقارَنةً مع الأماكن التي عُلِّقت فيها مُلصقات كبيرة لأزهار أو أشياء أخرى لطيفة. في العام التالي، علّقت مجموعة مماثلة من الباحثين في الجامعة لافتات قرب مناصب الدراجات الهوائية حول الحرَم جاء فيها، "يا لصوص الدراجات: نحن نراقبكم"، مع نص مطبوع فوق صورة فوتوغرافية لعينَين بشريّتَين. فانخفض عدد سارقي الدراجات بنسبة 62 في المئة في الأماكن حيث عُلّقت اللافتات الجديدة، ولكنها ازدادت في المواقع حيث لا وجود للافتات (بنسبة 65 في المئة)، مما يوحي بأن اللصوص نقلوا نشاطاتهم إلى أماكن أكثر أمناً. كتب الباحثون "توحي فعالية هذا التدخل البسيط والرخيص إلى أبعد حد بإمكانية وجود منافع كبيرة جرّاء تخفيض مستوى الجريمة لدى اعتماد سيكولوجيا الرَّقابة، حتى بغياب الرَّقابة ذاتها".

يحمل مسرحُ الرَّقابة - التظاهر بممارسة الرَّقابة من خلال عيون بشر أو روبوتات - الناسَ، في الواقع، على معاملة أحدهم الآخر بشكل أفضل. ولكن لا قرار حاسم بعد في شأن ما إذا كانت الرَّقابة الممارَسة عبر الكاميرات تردع الجريمة.

لقد وجد تحليل أجرته دائرة الأبحاث في كاليفورنيا عام 2008 على أربعة وأربعين دراسة عن البثّ التلفزيونيّ المُغلَق (CCTV) أن 43 في المئة من الدراسات لم تُظهر أي تأثير لهذا البث على الجريمة، في حين أن 41 في المئة أظهرت انخفاضاً هاماً للجريمة على الصعيد الإحصائي.

وفي العام 2011، حلّل المعهد المدينيّ أنظمة رَقابة بواسطة الكاميرات في بالتيمور في شيكاغو، وواشنطن العاصمة، وجاءت النتائج متضاربة على نحو مماثل. في بالتيمور، وجد المؤلّفون أن شبكة من خمسمئة كاميرا، يقوم فريق ضباطِ شرطة متقاعدين ومدرَّبين بمراقبتها على مدار الساعة، أسهمت بانخفاض الجريمة ككل بنسبة 35 في المئة في الشهر في حيّ واحد. ولكن

ثبت أن كاميرات في أحياء أخرى كانت أقل نجاحاً. بصورة مماثلة، وجد المعهد المَدينيّ في شيكاغو، التي اعتمدت برنامج رَقابة تبلغ كلفته عدة ملايين من الدولارات مع أكثر من ثمانية آلاف كاميرا، أن الكاميرات أسهمت بانخفاض الجريمة في هامبولت بارك بنسبة 12 في المئة، ولكنه لم يلحظ أي انخفاض هام في الجريمة، على الصعيد الإحصائي، في غارفيلد بارك الغربي. وفي واشنطن العاصمة، وجد المعهد المَدينيّ أنه لم يكن لكاميرات الرَّقابة أي تأثير هام على الجريمة، على الصعيد الإحصائي.

هناك سبب واحد للنتائج المتضاربة: قد تساهم عدة عوامل في انخفاض الجريمة، ويصعب عزل رَقابة الكاميرات عن عوامل أخرى، كدوريات الشرطة المتزايدة أو الإضاءة المحسَّنة.

في العام 2004، حلّل ليون همبل وإريك توبفر، وهو مؤلّف يعمل في مركز التكنولوجيا والمجتمع في برلين، دراسات عن استخدام البثّ التلفزيوني المُغلَق في أوروبا، ووجدا أن دراسات عديدة تفتقر إلى مجموعات ضبط كي تتمّ المقارنة بين تطوّر الجريمة في المناطق حيث ثُبّتت كاميرات وتطوّر الجريمة في المناطق الأوسع التي لا تحتوي على كاميرات، وتفتقر إلى تحليل يتناول انتقال الجريمة من المناطق التي شملتها الدراسات إلى مناطق أخرى.

وتُظهر الدراسات القليلة التي استخدمت مجموعات ضبط وجود دعم قليل للنظرية القائلة إن باستطاعة الكاميرات منع الجريمة. وأظهرت دراسة أخرى للمعهد المَدينيّ جرت عام 2011، وحلّلت تأثير كاميرات الرَّقابة على الجريمة في مواقف السيارات - واستخدمت طريقة اختبار عشوائية مضبوطة - أن الكاميرات لم تُحدث فَرقاً حقيقياً. وقارنتِ الدراسةُ الجريمةَ المرتبطة بالسيارات المرتكَبة في عام واحد في خمسة وعشرين موقف سيارات قرب محطات قطار الأنفاق في واشنطن العاصمة التي ثبّتت كاميرات تنشط بالحركة، مع جرائم مماثلة في خمسة وعشرين موقف سيارات لا تحتوي على كاميرات. وبالرغم من كونها كاميرات رقمية ثابتة، أشار الباحثون إلى دلالات تعطي الانطباع بوجود رَقابة متواصلة في موقف السيارات بواسطة كاميرات. ووجدت الدراسة أن "لا أثر مميَّز للكاميرات على الجريمة".

وهناك ما يشير إلى أن أضواء الشارع البسيطة قد تمنع الجريمة بقدْر كاميرا الرَّقابة. ففي العام 2004، حلّل الخبيران الجنائيان براندون وِلش وديفيد فارينغتون اثنتَين وثلاثين دراسة أجرتها الولايات المتحدة، كندا، وبريطانيا، لتحديد ما إذا كان البثّ التلفزيوني المُغلَق يمنع الجريمة بفعالية أكبر من أضواء الشارع البسيطة. وجاء الاستنتاج كالتالي: أضواء الشارع

والبثّ التلفزيوني المُغلَق متساويان بالفعالية لمنع جرائم المِلكيات - وأيّ من الوسيلتَين ليس جيداً بما يكفي لمنع الجرائم العنيفة. ووضعا النظرية القائلة إن الكاميرات وأضواء الشارع "هما وسيلتان تحفيزيتان تحثان على تخفيض الجريمة عبر إحداث تغيير في الإدراك الحسّي للسكان والمسيئين المحتملين، وموقفهم، وسلوكهم".

وخمّن مؤلّفو دراسة المعهد المَدينيّ أن تكون الكاميرات فعالة فقط عندما تكون مضبوطة من قِبَل عملاء إنفاذ القانون الذين يتصرفون بسرعة وفقاً للمعلومات التي يتم تلقّيها من الكاميرات. "التكنولوجيا جيدة فقط بجودة طريقة استخدامها"، كتبوا.

بمعنى آخر، يتمثل عمل كاميرات الرَّقابة بالتأثير في السلوك البشري عندما يقتنع الناس فقط بوجود شخص في الجانب الآخر للكاميرا يقوم بمراقبتهم.

á á á

من غير الواضح أيضاً ما إذا كانت الرَّقابة من خلال تحليل بيانات كمبيوترية مساعِدةً لإلقاء القبض على إرهابيين قبل القيام بهجومهم.

بالرغم من كل شيء، أفلتت العديد من المكائد الإرهابية من رَقابة شبكات التعقُّب. فمنذ 11/9، حدثت سلسلة من الهجمات الإرهابية، وفي ما يلي أبرزها:

- **مرتكب عملية تفجير بواسطة الحذاء.** عام 2001، حاول ريتشارد كولفين ريد تفجير عبوة ناسفة في حذائه في رحلة جوّية من باريس إلى ميامي، وأخفقت محاولته.
- **مُطلق النار في مطار لوس أنجلوس الدولي.** عام 2002، فتح هشام محمد هدايت، وهو مصري، النار على منضدةِ تذاكر لشركة طيران العال في مطار لوس أنجلوس الدولي، قاتلاً شخصَين ومصيباً آخرين بجراح.
- **مُطلق النار في فورت هود.** عام 2009، دخل الرائد في الجيش الأميركي، نضال مالك حسن، مركزاً للتعبئة في فورت هود في تكساس، وقفز على طاولة وصاح "الله أكبر"، وفتح النار بواسطة مسدّسَين. فقتل ثلاثة عشر شخصاً وأصاب ثلاثة وأربعين آخرين بجراح.
- **مرتكب عملية تفجير بواسطة ملابسه الداخلية.** في يوم الميلاد عام 2009، حاول عمر فاروق عبد المطّلب تفجير عبوات ناسفة مُخاطة في ملابسه الداخلية على متن رحلة جوّية من أمستردام إلى ديترويت. لم ينفجر الجهاز بل اشتعل ببساطة - مُصيباً عبد المطّلب وراكبَين آخرَين.

- **مفجّر تايمس سكوير.** عام 2010، حاول فيصل شهزاد، الذي كان قد تلقّى تدريباً مع إرهابيين في باكستان، تفجير عبوة ناسفة مزروعة في سيارة في تايمس سكوير في نيويورك، ولكنه أخفق.
- **مفجّرا ماراتون بوسطن.** عام 2013، وضع تامرلان وجوهر تسارناييف، كما زُعِم، عبوات ناسفة من صنع منـزليّ قرب خط النهاية لماراتون بوسطن. أصابت الانفجارات مئات الأشخاص بجراح، وقتلت ثلاثة أشخاص بمن فيهم فتى في الثامنة من العمر.

يشير مؤيّدو الرَّقابة إلى أن هذه الإحصائيات لا تأخذ بعين الاعتبار الهجمات التي تمّ منعها - يبقى العديد منها سرّياً. ومع ذلك، نملك للمرة الأولى دليلاً عن هجمات صُدّت.

فصبيحة تسريبات سنودن، كشف الجنرال كيث ألكسندر، مدير وكالة الأمن القومي، عن مساهمةِ شبكات التعقُّب عبر الهاتف والإنترنت المثيرة للجدل التابعة للوكالة "في فهمنا للمكائد الإرهابية، وساعدت في حالات عدة على إيقاف هذه المكائد" في أربع وخمسين حالة.

لم يشر إلى الحالات بالتحديد - بالرغم من قوله إن معظمها أجنبيّ - ولكنه لم يخصّ بالذِّكر حالة نجيب الله زازي. ففي العام 2009، اعتُقل زازي قبل أيام من قيامه ورفاقه بالتخطيط، كما زُعم، لتنفيذ عملية تفجير انتحارية في نفق مدينة نيويورك.

وفقاً لألكسندر، جُرفت معلومات عن زازي متوافرة على شبكة تعقُّب تدعى عملية المبنى الشاهق. وعثرت وكالة الأمن القومي على رسائل بريد إلكتروني موجَّهة من زازي وسط رسائل متبادَلة بين الولايات المتحدة وباكستان كانت الوكالة تراقبها على شبكة التعقُّب بريسم التي تجرف رسائل البريد الإلكتروني الدولية المرسَلة إلى الولايات المتحدة.

ضمن تلك الاتصالات، عثرت وكالة الأمن القومي أيضاً على رقم هاتف. واستخدمت بعد ذلك شبكة باتريوت أكت المتعقِّبة لكل الاتصالات الهاتفية التي تُجرى في الولايات المتحدة لتحديد موقع أرقام أخرى متصلة بالرقم الأول. قال ألكسندر: "عثرنا على زازي يتحدث إلى رجل في نيويورك لديه صِلات بعناصر إرهابية أخرى".

عندما تمّ تنبيه الأف بـي آي، استخدم عملاؤها تقنيات إنفاذ القانون التقليدية. وتبعوا زازي أثناء قيادته إلى مدينة نيويورك من منـزله في كولورادو. عندما وصل، طلبت الأف بـي آي من سلطة الميناء اعتقال زازي عند نقطة تفتيش على جسر جورج واشنطن، ولكن لم يتم العثور على أي

شيء في سيارته. وسُمح لزازي بمواصلة طريقه، ولكنه رُوِّع بالرَّقابة. بعد أيام قليلة، عاد جوّاً إلى دِنفر دون تنفيذ مكيدته.

اعتُقل زازي في كولورادو، واعترف في وقت لاحق بذَنْبه في التُّهَم الموجَّهة إليه، بما في ذلك مؤامرة لاستخدام أسلحة دمار شامل، وتوفير دعم مادّي للقاعدة. لم يُحكَم عليه بعد.

ولكن من غير الواضح ما إذا كانت الحكومة بحاجة إلى شبكات تعقُّب للإيقاع بزازي. لو كان زازي يتبادل رسائل بريد إلكتروني مع إرهابيين خاضعين للرَّقابة، لَكانت مذكرة تفتيش كافية للحصول على اتصالاته. بشكل مماثل، عندما يتم تحديد رقم هاتفه، يكفي أن يقوم قاضٍ بالموافقة على سحب سجلات الاتصالات الهاتفية لذلك الهاتف.

عندما سأله مجلس الشيوخ عما إذا كانت شبكات التعقُّب "حاسمة" للإيقاع بزازي، راوغ الجنرال ألكسندر. لقد قال إن سجلات الهاتف غير حاسمة، ولم يُجب عما إذا كانت شبكات تعقُّب البريد الإلكتروني حاسمة للإيقاع بزازي. حتى إن الرئيس أوباما كان فاتراً لدى وصف استخدام شبكات التعقُّب الأميركية للإيقاع بزازي. "كان بإمكاننا الإيقاع به بطريقة أخرى"، قال في مقابلة تلفزيونية مع تشارلي روز. "ولكن على الهامش، نحن نـزيد فُرصنا لمنع حدوث كارثة مماثلة من خلال هذه البرامج".

هل الرَّقابة الجماعية جديرة بالمحاولة عندما يكون بإمكان مؤيِّديها الأكثر تحمّساً القول إنها "ساهمت في فهمنا" للحالات "على الهامش"؟

á á á

إن شبكات التعقُّب سيف ذو حدَّين أيضاً. فإذا كانت وكالات الاستخبارات تحصل على دليل دون أن تتتبّعه، فهي غالباً ما تتلقّى اللوم في حال وقوع هجوم. هذا ما حدث في حالات مرتكب عملية تفجير بواسطة ملابسه الداخلية، ومُطلق النار في فورت هود، ومفجّرَي ماراتون بوسطن. كان المرتكبون قد اعتُبروا بأجمعهم تهديدات إرهابية قبل شنّ هجماتهم.

في كتابهما أعداء الداخل: داخل وحدة التجسس السرّية في قسم شرطة نيويورك ومكيدة بن لادن الأخيرة ضد أميركا ، يؤرّخ الصحافيان مات أبوتزو وأدام غولدمان كيفية إخفاق رَقابة قسم شرطة نيويورك غير المميِّزة، التي تستهدف المسلمين في مدينة نيويورك، في الإيقاع بنجيب الله زازي وأصدقائه عندما كانوا يحلمون بمكيدتهم الإرهابية في كوينـز. كان باحثو قسم شرطة نيويورك قد راقبوا المطاعم في حيّ زازي، ومسجده، لا بل

أيضاً وكالة السفر حيث يشتري تذاكر رحلاته الجوّية إلى باكستان. "بعد سنوات من البحث، عرف قسم شرطة نيويورك أين كان مسلمو نيويورك"، كتب أبوتزو وغولدمان. "ولكنهم ما يزالون لا يعرفون أين كان الإرهابيون".

كان والد عمر فاروق عبد المطّلب، مرتكب عملية تفجير بواسطة ملابسه الداخلية، قد حذّر السفارة الأميركية في نيجيريا من وجهات نظر ابنه الراديكالية، ومن اختفاء ابنه وإمكانية سفره إلى اليمن. ووجد تحقيق أجراه البيت الأبيض أن "عدة وكالات" حصلت على معلومات عن عبد المطّلب قبل محاولة الهجوم، ولكنها لم تضعه على قائمة المراقبة.

كان مكتب ميداني تابع للأف بـي آي يراقب اتصالات مُطلق النار في فورت هود، نضال مالك حسن، برجل الدين أنور العولقي، ولكن المكتب لم يقم بأي عمل إضافي قبل فتح حسن النار في فورت هود. وكان مفجِّر ماراتون بوسطن المستقبلي، تامرلان تسارناييف، في قاعدة بيانات المركز القومي الأميركي لمكافحة الإرهاب قبل عام على الأقل من هجومه.

يقترح أحد الأبحاث أن جمع مقدار كبير من البيانات لا يمكنه ببساطة التوقع بأحداث نادرة كالإرهاب. لقد استنتجت وثيقة تعود للعام 2006 وضعها جيف جوناس، وهو عالِم في مركز أبحاث آي بـي أم، وجيم هاربر، مدير سياسة المعلومات في معهد كاتو، أن الأحداث الإرهابية غير كافية لتكون ملائمة لاستخراج بيانات كمبيوترية على نطاق واسع.

بالرغم من كل شيء، كان زازي يشتري مزيل طلاء أظافر لصنع متفجرة من الأسيتون، وكان عبد المطّلب يخيط متفجرات داخل ملابسه الداخلية، ويوجّه حسن رسالةَ مُعجَبٍ بالبريد الإلكتروني للعولقي. فلكل حدث أنماطه المتميّزة. بالمقارنة، إن استخراج البيانات جيّد في تتبّع بطاقة ائتمان واحتيال تأمينيّ في زمن يكون فيه الاحتيال أكثر شيوعاً. فشركات بطاقات الائتمان تطوّر رايات حمراء - عمليات تجارية في بلدان أجنبية، على سبيل المثال، يمكنها تحذيرهم من احتيال محتمَل. "بخلاف عادات المستهلكين التسوّقية والاحتيال المالي، لا يتكرر الإرهاب بما يكفي للسماح بوضع نماذج تنبّؤية صالحة"، استنتج جوناس وهاربر.

وفي العام 2008، دعت الأكاديمية الوطنية للعلوم عشرات الخبراء إلى اجتماع بهدف دراسة عملية استخراج البيانات لمكافحة الإرهاب. لقد توصّلت المجموعة إلى استنتاج مماثل: "لا يمكن تطبيق الأدوات والتقنيات المؤتمَتة إلى حد كبير على المسألة الأكثر صعوبة المتمثلة بالكشف عن هجوم إرهابـي واستباقه، وقد لا يكون النجاح في القيام بذلك ممكناً أبداً".

لقد ألمح بعض مسؤولي الاستخبارات إلى تَشاطُرهم التشاؤم نفسه في شأن قدرتهم على فرز مقادير كبيرة من البيانات للتنبّؤ بالهجوم التالي. ففي خُطبة ألقاها عام 2012، مدير المركز القومي الأميركي لمكافحة الإرهاب، قال ماثيو أولسن: "إذا حدث هجوم آخر، قد يكون من المحتمل أن تتمكنوا من العودة إلى الوراء واكتشاف إلماعة أو دليل ما في المقدار الكبير من البيانات التي ولجناها".

وبعد تفجيرات ماراتون بوسطن، ذهب مفوّض شرطة المدينة، إِد ديفيس، إلى أبعد من ذلك، قائلاً للكونغرس إن رَقابة أكثر اعتماداً على التكنولوجيا ما كانت لِتساعده. "لا وجود لأي كمبيوتر يستطيع الإخبار عن اسم إرهابـي"، قال، بل إن أفضل الأدلة تأتي من أشخاص يحذّرون "سلطات إنفاذ القانون عندما يتم اكتشاف انحراف ما. نحن بحاجة إلى حدوث ذلك، ويجب أن تكون خطوتنا الأولى".

á á á

إذاً، ماذا يمكننا الاستنتاج من حياة تشهد حالة من الرَّقابة؟

يوحي الدليل أن باستطاعة الرَّقابة البشرية، أو الرَّقابة عبر صور عيون بشرية أو كاميرات يراقبها الناس بشكل فعال، تعديل السلوك لتعزيز عادات اجتماعية إيجابية، كإفراغ الأطباق من فضَلات الطعام في كافتيريا مشترَكة، وصدّ جرائم مرتبطة بالمِلكية أحياناً. من جهة ثانية، هناك دليل يوحي بأن إضاءة الشارع يمكن أن تكون فعالة أيضاً. وساعدت الرَّقابة المتبادَلة، كما يبدو، على منع حدوث دمار متبادَل مؤكَّد أثناء الحرب الباردة.

مع ذلك، لا يبدو أن الرَّقابة جيدة للتنبّؤ بالإرهاب بسبب إفلات العديد من الأحداث الإرهابية من شبكات التعقُّب. حتى إن الشتازي أخفقت في التنبؤ بانهيار النظام الألماني الشرقي عام 1989. وقد يكون دفق البيانات الناجمة عن الرَّقابة غامراً ومُربِكاً لأولئك المسؤولين عن فرزها للعثور على إرهابيين.

ولكن الرَّقابة العلنية كلّية الوجود تبدو جيدة لممارسة القمع. لقد تبيّن أن الأشخاص الذين خضعوا للمراقبة بطريقة سرّية غير مميِّزة - سواءً في ألمانيا الشرقية أو في الدراسة الفنلندية - كانوا يراقبون سلوكهم وكلامهم.

ويصبح السؤال إذاً: هل فوائد الرَّقابة كلّية الوجود وغير المميِّزة التي تمارسها شبكات التعقُّب جديرة بمحاولة العيش في ثقافةِ خوف؟

الفصل الرابع
حرّية الاشتراك في الجمعيات

لم يَعُد ياسر عفيفي يؤمن بالصُّدف. فإذا رأى السيارة نفسها مرتَين أثناء القيادة، يتوتّر ويفكّر ملياً في تغيير طريقه. "أتفحّص الأمور التي تحدث بالصَّدفة كعالِم"، يقول. لم يُصَب ياسر بالذُّهان الارتيابـي بشكل طبيعي. فطبعه متفائل، ومشيته نشيطة، ومصافحته ثابتة. في سنّ الثالثة والعشرين، هو يُظهر التفاؤل الأزلي لبائعٍ حديث العهد. ولكن منذ اكتشاف ياسر أنه مراقَب من قِبَل الأف بـي آي، أصبح حذراً للغاية.

غادر ياسر منـزله - الذي كان يتشاطره مع ثلاثة أصدقاء عازبين - وتزوّج بامرأة لديها ابنتان من زواج سابق. يقضي الأمسيات في المنـزل، مساعداً الفتيات في فروضهما المنـزلية. لقد توقف عن استخدام فيسبوك إلا لممارسة قليل من الألعاب. يقول ياسر: "أنا أحد أولئك الأشخاص الذين يعتقدون أن كل ما تطبعينه على شبكة الإنترنت أو تقولينه على الهاتف يذهب إلى قاعدة بيانات".

هو يتجنّب الأحاديث التي تتناول السياسة أو الدين. لقد بدأ باستخدام اسم مختلف في العمل، علاء الدين، لأنه لم يشأ قيام رب عمله بالبحث عنه على الغوغل ورؤية خبر الرَّقابة التي تفرضها عليه الأف بـي آي. هو لا يُظهر أي حسّ فكاهة حيال المقالب التي تخرق القانون. فإذا اقترح عليه صديق إطلاق دُعابة للإيقاع بضحيّةِ كِذبة نيسان/أبريل، يقول، "أُجيبه، ما تقوله خاطئ، إنه غير قانوني". وحتى ولو قالوا إنها مجرد دُعابة، أقول، أَلغوا رقم هاتفي". يقدِّر أنه كفّ عن التسكّع مع نحو 90 بالمئة من أصدقائه السابقين الذين "يحبون أن يثملوا ويقوموا بأمور غبية"، يقول. نادراً ما يتحدث إلى صديقه المفضَّل منذ سنّ الطفولة الذي ينشر على الإنترنت قيامه بتدخين الماريجوانا، ويقضي وقت فراغه على ألعاب فيديو.

أثناء غداء متمهّل في مطعم هندي مع ياسر وزوجته، أنجلينا عصفور، سألتها عن مدى تغيّره منذ إخضاعه للرَّقابة. فقالت لي، "هو نفسه في الأساس. ليس لديه أيّ من الأصدقاء أنفسهم".

وأضاف ياسر: "لقد جعلني الأمر حذراً حقاً ممن أكون على صِلة بهم".

á á á

إن تصنيف الأشخاص وفقاً لصِلاتهم هو تكتيك مفضَّل لدى الأنظمة القمعية. كان يتملك الشتازي هاجس تحديد هوية كل من يكون على صِلة بألمانيا الغربية، ويتملك النازيين هاجس تحديد هوية كل من يحمل دماً يهودياً. ويتملك الإيرانيين هاجس تحديد هوية كل من يكون على صِلة بالولايات المتحدة. ويتملك الصينيين هاجس تحديد هوية أية معارضة محتمَلة للحُكم.

لهذا السبب، إن حرّية إقامة الصِّلات هي أحد الحقوق الواردة في الإعلان العالمي لحقوق الإنسان الصادر عن الأمم المتحدة الذي تمّ تبنّيه بعد الأعمال الوحشية التي شهدتها الحرب العالمية الثانية.

بصورة عامة، تعني حرّية إقامة الصِّلات عدم منع الناس من الانضمام إلى مجموعات أو إرغامهم على الانضمام إلى مجموعات. في الولايات المتحدة، منح التعديل الأول الذي يحمي حرّية التعبير وحرّية التجمّع حق إقامة الصِّلات أيضاً.

في العام 1958، تَمثّل الحكم الصادر عن المحكمة العليا بعدم دستورية محاولة ولاية ألاباما الحصول على قوائم عُضوية الجمعية الوطنية لتَقَدّم الشعب الملوّن لأنها قد تجمّد حق الأعضاء بإقامة صِلات وفقاً للتعديل الأول، وذلك الحق أساسي للحرّية التي يَعِد بها التعديل الرابع عشر. "إن الكشف عن هوية أعضائها من عامة الناس عرّض هؤلاء الأعضاء إلى إجراءات انتقامية اقتصادية، وفقدان وظائفهم، والتهديد بالإكراه البدني، ومظاهر أخرى من العداء العام"، كتب رئيس المحكمة العليا جون مارشال هارلن في رأيه القضائي الذي وافق عليه أكثر من نصف أعضاء المحكمة. "في ظل هذه الظروف، نعتقد أن الإرغام على الكشف عن عُضوية الملتمِس في ألاباما قد يؤثر بشكل معاكس، على الأرجح، في قدرة الملتمِس وأعضائه على مواصلة جهدهم الجماعي لتطوير معتقدات يحق لهم مناصرتها، وهو أمر مُعترَف به".

ولكن في عالم اليوم، إن فكرة حماية أفراد جماعة فقط هي طريقة قديمة الطراز لأخذ فكرة عن حرّية إقامة صِلات. لم يكن يتعيّن على ياسر الانضمام إلى مجموعة مثل مسلمو سانتا كلارا الشبان كي تلاحظ السلطات إقامته صِلات. لقد أشار تتبع مساره الرقمي إلى إقامته صِلات يمكن للأف بـي آي غرفها بقليل من الجهد.

في الواقع، يمكن القول إن الهدف من اعتماد قدْر كبير من

التكنولوجيا في هذه الأيام كشْفُ النقاب عن صِلاتنا المحجوبة. تأمّلوا بالأشخاص الذين يتتبّعون تحركاتهم الخاصة باستخدام عدّاد الخُطى فِيبيت وأدوات أخرى لهذه التكنولوجيا - هم يدرسون تحركاتهم الخاصة بهدف فهم الصِّلات المحجوبة بشكل أفضل. هل يشعرون بحال أفضل في بعض الأيام لدرجة سيرهم أكثر من أيام أخرى؟

تأمّلوا بزوجي الذي ثبّت أجهزة تحسّس في جدراننا بهدف مراقبة استخدامنا للكهرباء، والغاز، والماء. هو يحاول كشف النقاب عن الصِّلات المحجوبة. ونجح الأمر: نعرف الآن أن محمصة الخبز الكهربائية غير فعالة بشكل لا يصدَّق وأن استخدامنا للماء مُحبِط بشكل غريب. (أُلقي اللوم على اغتسالات ابني الطويلة، ولكننا لم نجمع البيانات تماماً لنُثبت ذلك بعد).

أنا متحمسة للتعلّم من بياناتي، ولكن التكنولوجيا نفسها التي كنا نستخدمها لمراقبة أنفسنا يستخدمها آخرون أيضاً لمراقبتنا ولوضع ملفات عن أشيائنا المفضَّلة وغير المفضَّلة، وعن صِلاتنا.

في عالم اليوم، يضعنا كل خيار نتخذه في صِلة مع شخص، مكان، أو فكرة. زوروا موقعاً سياسياً على الويب: أنتم على صِلة بوجهات نظره. اجلسوا في مطعم قرب شخص ما مراقَب: هاتفكم المحمول هو الآن جزء من المجموعة المثيرة للاهتمام التي يمكن أن تكون مراقَبة من قِبل السلطات. تُعرَف تلك الصِّلات وتدخل قواعد بيانات حيث يستخدمها الناس لوضع توقعات حول السلوك المستقبلي.

حتى إن مؤيِّدي ما يدعى حركة بيانات ضخمة يُقِرّون بأن هذه المسائل معقَّدة. في كتابهما العائد للعام 2013 بيانات ضخمة: ثورة ستحوّل طريقة عيشنا، وعملنا، وتفكيرنا ، يقول فيكتور ماير شونبرغر وكينيث كوكيار إنه باستخدام بيانات كبيرة بشكل متزايد لوضع توقعات عن سلوك الناس، يتعيّن تثبيت وسائل حماية في الموضع الصحيح تستلزم على الأرجح استحداث مهنة جديدة تدعى وضع خوارزميات تسمح بالتدقيق باستخدام بيانات ضخمة. "بدون وسائل الحماية هذه، قد تتقوّض فكرة العدالة ذاتها"، كتبا.

ويحذّر إريك شميت، رئيس غوغل ومؤيّد البيانات الضخمة، في كتابه العصر الرقمي الجديد الذي وضعه بالتعاون مع جارد كوهين، من أن نشوء "تخزين للبيانات بشكل دائم تقريباً" يبشر باقتراب حقبة "يُحمَّل فيها الناس مسؤولية صِلاتهم الفعلية في الماضي والحاضر". فبالرغم من كون شميت

وكوهين متفائلَين في الغالب حيال كيفية قيام التكنولوجيا بمساعدة المواطنين، هما يحذّران في قسم من الكتاب يدعى "الدولة البوليسية 2,0" من أن "كل ما يحتاج إليه نظام ما لإنشاء دولة بوليسية رقمية مرعبة بشكل لا يصدَّق متوافرٌ الآن تجارياً". في ظل سيطرة دولة بوليسية، يكتبان، "سيحمل الذَّنْبُ بسبب الصِّلات معنى جديداً مع هذا المستوى من المراقبة".

á á á

بدأت رَقابة ياسر عفيفي، كما يبدو، بسؤال بريء عن سبب عدم إمكانية تمرير مزيل الرائحة عبر جهاز الكشف في المطار.

ففي 24 حزيران/يونيو 2010، نشر مستخدم لموقع التواصل الاجتماعي Reddit.com ، ويدعى جاي كلاي، سؤالاً: "إذاً، إذا كان بإمكان مزيل رائحتي أن يكون متفجّرة، لماذا ترمونه في وعاء القمامة؟"

لقد ولّد تصريحه مئات التعليقات. ودعا بعض مستخدمي Reddit الحظرَ الذي يطال مزيل الرائحة "مسرح الأمن". وتحدّث آخرون عن سِلع قاموا بنقلها سرّاً إلى متن الطائرات - مِقصّ أظافر، إبر خيزران، آلات حلاقة، سكاكين. واقترح أحد المستخدمين أن مركز التسوّق هو هدف أسهل للتفجير .

في 25 حزيران/يونيو، تدخّل مستخدم يدعى خالد الغجري: "يبدو تفجير مركز تسوّق أمراً سهلاً"، كتب. "أعني أن كل ما تحتاجون إليه هو متفجرة، وبِذلة عادية كي لا تكونوا الشخص المجنون في مِعطف الذي يحاول تفجير مركز تسوّق وحقيبة تسوّق. أعني أنه إذا كان الإرهاب تهديداً منطقياً في الواقع، فكّروا في عدد مراكز التسوّق التي كانت لِتتعرّض للتفجير".

واختتم خالد الغجري بدُعابة من نوع ما: "... إذاً... أجل... لقد تم التسلل إلى ملفاتي بالتأكيد".

كان خالد الغجري خالد إبراهيم في الواقع، وهو طالب في سانتا كلارا، كاليفورنيا، في التاسعة عشرة من العمر والصديق المفضَّل لياسر عفيفي. فخالد دقيق دون أن يعي ذلك. وبعد أربعة أشهر، ذهب مع ياسر لتغيير زيت محرك سيارة ياسر، وهي لينكولن زرقاء أل أس 2000 صالون. عندما رُفعت السيارة، لاحظ ياسر سلكاً مدلّى من عجلات الهبوط متصلاً بما بدا أشبه براديو إرسال واستقبال عملاق مثبّت بأسفل سيارته.

"هذا ليس جزءاً من السيارة"، قال ياسر للميكانيكي.

وعندما سحب الميكانيكي الجهاز، اقتُلع بسهولة؛ كان ملتصقاً بواسطة

مغناطيس. فقال ياسر لنفسه: "إما يكون جهازَ تعقُّب قديم الطراز جداً أو يُفترض به أن يبدو كقنبلة أُنبوبية".

وُلد ياسر ونشأ في سانتا كلارا، وكان قد انتقل إلى مصر مع والده المصريّ المولد، عندما كان في الثانية عشرة من عمره، بعد انفصال والدَيه. عندما بلغ الثامنة عشرة من العمر، عاد إلى الولايات المتحدة ليرتاد الكلية، ويحصل على وظيفة، ويعيش بمفرده. كان ياسر وخالد، وعائلة هذا الأخير مصرية أيضاً، صديقَين مقرَّبين جداً في المدرسة الإعدادية، وعادت صِلتهما السابقة عندما عاد ياسر إلى الولايات المتحدة.

بعد قليل من عودة ياسر إلى الولايات المتحدة، يقول، ظهر عميل أف بـي آي عند بابه عندما كان خارج المنـزل، وترك بطاقة تطلب منه الاتصال. عندما اتصل ياسر، قال له العميل إن الأف بـي آي تريد التحدث إليه "لأننا تلقّينا معلومة مجهولة المصدر تقول إنك ربما تكون تهديداً للأمن القومي". قال ياسر إنه يسرّه الإجابة عن الأسئلة، ولكنه يريد أولاً استشارة محامٍ.

اتصل ياسر بخدمة قانونية مُسبَقة الدفع نصحته بعدم التقاء العميل. لذلك، رفض دعوة الأف بـي آي ونسي أمرها. وانكبّ على صفوف إدارة الأعمال وعلى وظيفته المتمثلة ببيع تجهيزات كمبيوترية لشركات في الشرق الأوسط.

ولكن بعد اكتشافه الجهاز المزروع تحت سيارته، فكّر مجدداً في الأف بـي آي. فرمى الجهاز على المقعد الخلفي وعاد إلى المنـزل ليُريه لزملائه في السكن.

لقد شعر أحد زملائه في السكن بالقلق لأن الجهاز يشبه متفجرة. فتساءل ياسر عن المبلغ الذي سيتقاضاه لقاء بيعه. واقترح خالد، الأكثر ارتياباً في طبعه، نشر صورة الجهاز على Reddit أولاً لمعرفة ماهيّته. وهكذا، عند الساعة العاشرة والربع صباحاً، أدخل خالد صورة للجهاز إلى Reddit مع سؤال بسيط: "هل يعني هذا أن الأف بـي آي تلاحقنا؟"

عند منتصف الليل، كان المعلّقون على Reddit قد عرفوا الجهاز: إنه نظام تحديد المواقع العالمي غارديان أس تي 820 الذي تنتجه كوبهام، وهي شركة تبيع وتسوّق منتجاتها لوكالات إنفاذ القانون حصراً. باختصار: "أجل، الأف بـي آي أو الشرطة تلاحقك"، كتب المستخدم jeanmarcp .

في بادئ الأمر، شعر ياسر بالحماسة. لقد نُشر الإعلان في الصفحة الأمامية لـ Reddit ، وعلّق أكثر من ثلاثة آلاف شخص على الفِقرة، وانهالت

عليه النصائح من كل حَدْب وصَوْب. وتذكّر ياسر تفكيره في أن "الأمر مثير للرَّهبة".

في اليوم التالي، بدأت حماسته بالتلاشي. فقال له زملاؤه في السكن إن رجلاً وامرأة كانا واقفَين بجانب سيارته في موقف سيارات المجمَّع السكني. متظاهراً بالشجاعة، نـزل ياسر لمواجهتهما. كانا ما يزالان واقفَين بجانب سيارته المركونة داخل بوّابات إلكترونية تتحكم بولوج مجمَّعه السكني. "مرحباً، هل يمكنني مساعدتكما بشيء؟" سأل ياسر. "أنتما تقفان بجانب سيارتي تماماً".

"هل تعرف أن لوحاتك المعدنية انتهت مدة صلاحيتها؟" قال الرجل، مُطلقاً ضحكة.

"ما شأنك في ذلك؟" سأل ياسر. "رجاءً، ابتعد عن سيارتي أثناء تحريكها إلى الخلف".

للحظة من الزمن، بدا الأمر كما لو أن ياسر سيترك الغريبَين وراءه. فانطلق خارج المجمّع السكني وانعطف يساراً إلى الشارع. عندئذٍ، سمع صأي إطارات ورأى سيارتَين رباعيّتَي الدفع قاتمتَي اللون تندفعان خلفه. لقد تبعتاه مسافة نصف مجمَّع سكني، ومن ثم أرسلتا إشارات بأضوائهما. ورأى في مرآة الرؤية الخلفية انضمام سيارة ثالثة إليهما - شيفي كابريس سوداء.

فأوقف ياسر سيارته إلى جانب الطريق بعد قطع مئات قليلة من الأقدام. كان أمام المدرسة الإعدادية القائمة على الجانب الآخر من مجمّعه السكني. فسار ستة أشخاص نحو سيارته - الرجل والمرأة اللذان كانا بجانب سيارته، وأربعة عملاء يرتدون سترات لا يخترقها الرصاص ويحملون مسدسات.

لقد خفقت معدة ياسر وبردت يداه، ولكنه حاول أن يبقى متماسكاً. فعرّف أحد العملاء بنفسه بأنه "شرطي" وسأله عن لوحاته المعدنية المنتهية الصلاحية. "ألهذا السبب أوقفني جيش؟" أجاب ياسر. فسأله ضابط الشرطة إذا كان بإمكانه تفتيش السيارة، فأجاب ياسر بالإيجاب. ولكن بدلاً من تفتيش العربة، طلب الشرطي من ياسر الخروج من السيارة ومكالمة عملاء الأف بـي آي الواقفين وراء السيارة.

خرج ياسر من السيارة. فربّت الشرطي على ملابسه من الأعلى إلى الأسفل بحثاً عن سلاح، ومن ثم سمح له بالاقتراب من عملاء الأف بـي آي - الرجل والمرأة نفساهما اللذان كانا واقفَين بجانب سيارته في وقت سابق. فعرّف الرجل بنفسه، قائلاً إنه يدعى فينسنت، وتدعى المرأة جنيفر.

طالب فينسنت باستعادة جهاز التعقُّب. "لا أملكه"، قال ياسر. "كيف

تعرف أنني لم أبِعه؟"

تظاهر فينسنت بالقسوة، مُعلِناً أن الجهاز مُلك فيدرالي، ومهدداً بتوجيه تُهم فيدرالية ضد ياسر. "أعطنا الجهاز وإلا تعرّضتَ للاعتقال بتُهمة إعاقة العدالة"، هدّد فينسنت. فطلب ياسر الاستعانة بمحامٍ ولكنه لم يلقَ أية استجابة.

وتظاهرت جنيفر باللطف. "نريد فقط استرجاع الجهاز، أَعِده لنا فحسب فندعك وشأنك"، قالت.

اقترح ياسر أن يقوم محاميه بالاتصال بهم للقيام بالإجراءات لإعادة الجهاز. ولكن هذا الأمر أغضب فينسنت الذي صاح قائلاً إنه يجب على ياسر تسليم الجهاز على الفور.

"لماذا تفعلون بـي هذا؟" سأل ياسر.

فأخرج فينسنت ورقة تحمل إعلان خالد على Reddit الذي يتناول تفجير مركز تسوّق.

"لهذا السبب نتعقّبك"، قال فينسنت.

"لماذا لم تضعوا هذا الجهاز تحت سيارته؟" قال ياسر.

"أوه، أنتما معاً كل يوم"، قال فينسنت.

"إذاً، ما رأيك بما قاله؟" سألت جنيفر.

"إنه أمر شديد الغباء"، قال ياسر. "خالد شديد الذكاء، ولكن ما كتبه ينمّ عن غباء شديد... لماذا لا تذهبان للتحدث إليه؟"

في النهاية، بدأت صلابة ياسر بالانهيار في وجه الرجال المسلّحين. فوافق على إعادة الجهاز الموجود على الطاولة الصغيرة المنخفضة في شقته.

وعبر ياسر، جنيفر، وفينسنت، الشارع وعادوا إلى داخل المجمّع السكني، أثناء قيام أصدقائه وجيرانه بالمراقبة. وتبعهم العملاء الأربعة المسلّحون. فأدخلهم ياسر عبر البوّابات الإلكترونية، وصعدوا السلّم الخارجي إلى شقته في الطابق الثاني.

أثناء قيام ياسر بفتح قفل الباب، حاول فينسنت دخول الشقة معه. "ابتعد عن الباب"، قال ياسر.

كان زملاؤه في السكن يشاهدون التلفاز في غرفة الجلوس. "أيها الزملاء، الأف بـي آي خارج الباب"، قال لهم ياسر. وقبل أن تسنح لهم فرصة الإجابة، التقط الجهاز، واصطحبه إلى الخارج، وأعطاه لفينسنت.

"هل ستقوم باعتقالي؟" سأله ياسر.

"لا"، أجاب فينسنت. "ولكننا نرغب في طرح بضعة أسئلة عليك".

بعد أن أصبح جهاز التعقُّب بعيداً عن متناول يده، شعر ياسر بالفُضول لسماع المزيد عن مدى مراقبته من قِبَل الأف بـي آي. فوافق على إجراء محادثة وجيزة.

وعاد معهم إلى سياراتهم. فابتعد العملاء الأربعة بسيارتهم، تاركين ياسر بمفرده مع فينسنت وجنيفر التي أعطته بطاقة عمل تعرّف بأنها جنيفر كنعان، عميلة لدى الأف بـي آي.

وشرعا بإمطاره بأسئلة بدت كما لو أنها عن جهاد:

هل سافر إلى سوريا، إيران، أو أفغانستان؟ لا.

هل خضع لأي نوع من التدريب العسكري في الخارج؟ لا.

هل كان متديّناً؟ "أقصد المسجد يوم الجمعة"، قال ياسر.

فكتبت جنيفر على دفتر مدوّناتها، "ياسر عفيفي ليس تهديداً على الأمن القومي"، وأَرَتِ الصفحة لياسر.

الآن، حان دور ياسر لطرح أسئلة. "كيف لي أن أعرف أنكما لا تتبعانني إلى كل مكان؟" سأل.

فأجابت جنيفر باللغة العربية. "أحب حقاً ذوقك في المطاعم"، قالت.

فأُذهل ياسر. "تتكلمين العربية. هل تخدعينني؟" قال.

وتابعت بالعربية: "نعرف أين تذهب، نعرف ما تفعل، نعرف أنك تصطحب حبيبتك إلى سانتانا روو"، وهو مركز تسوّق في سان خوسية.

"واو، ماذا تعرفون أيضاً؟" سأل ياسر.

"نعرف أن لديك عمل جديد - تهانينا على عملك الجديد"، قالت. "نعرف أنك ستذهب إلى دُبَي بعد أسبوعَين".

فغاص قلب ياسر. لم يتحدث عن العمل إلا عبر الهاتف، ولم يناقش رحلة دُبَي إلا عبر رسائل البريد الإلكتروني. لا بد أن الأف بـي آي تُصغي إلى اتصالاته وتقرأ بريده الإلكتروني. فقال في نفسه: "هل تعرفون أيضاً ما هو لون سراويلي الداخلية؟"

"أنا واثق من أنكم تُصغون إلى اتصالاتي الهاتفية"، قال.

"أوه، لا يمكنني البوح بذلك"، أجابت.

"هل سأراكما ثانيةً؟ هل ستوقفانني ثانيةً مع جيشكما؟" قال ياسر.

"لا تقلق حيال هذا الأمر، أنت مُمِلّ"، قالت. "لن نـزعجك ثانيةً. لا حاجة للاتصال بمحامٍ".

لم يكترث ياسر بنصيحة الأف بـي آي. فبعد مغادرة العميلَين، وضعه أحد الأصدقاء على اتصال مع مجلس العلاقات الأميركية - الإسلامية، وهي

مجموعة دفاع مسلمة قانونية.

في 2 آذار/مارس 2011، تقدّم محامو المجلس بشكوى أمام محكمة فيدرالية، زاعمين أن نظام تحديد المواقع العالمي المتعقّب غير المُرفَق بمذكرة انتهك حقوق ياسر الواردة في التعديل الرابع، وأن وضع ملفات عن سلوكه الديني انتهك حقوقه الواردة في التعديل الأول، وأن الرَّقابة تسببت "بإحباط موضوعيّ حيال نشاطاته الواردة في التعديل الأول"، إضافةً إلى تُهَم أخرى.

زعمت الشكوى أن ياسر بات يشعر بالخوف "من التعبير عن وجهات نظره السياسية والاحتفاظ ببعض صِلاته القانونية" وأن الرقابة "منعت آخرين من إقامة صِلات به، ولا سيما مستخدِمين محتمَلين".

لم يسعَ ياسر إلى حكم قضائي ضد التعقُّب المستقبلي فقط، بل طلب أيضاً إلغاء البيانات المرتبطة بمكان إقامته من السجلات الحكومية.

فاز مكتب التحقيقات الفيدرالي بحق تقديم رد سرّي على شكوى ياسر. في مستنداته القانونية العامة، قال المكتب إن التحقيق الذي أجراه عن ياسر أُقفل وإن تعقُّب ياسر دون الحصول على مذكرة كان قانونياً في ذلك الوقت. (مذاك الحين، قالت المحكمة العليا إنه من غير المقبول قيام العملاء بانتهاك الحُرمات من خلال تثبيت نظام تحديد المواقع العالمي المتعقِّب). وجادلت الحكومة أيضاً، قائلةً إنه ليس باستطاعة ياسر الإشارة إلى أي دليل حسّي على الانتقاص من حقوقه الواردة في التعديل الأول في المستقبل: "لم يُثبت وجود تهديد حسّي وشيك بحدوث هذا الأمر في المستقبل".

á á á

التعديل الأول للدستور الأميركي حق سلبيّ. هو يذكر ما لا يمكن القيام به: " لا يصدر الكونغرس أي قانون خاص بإقامة دين من الأديان أو يمنع حرية ممارسته، أو يحد من حرية الكلام أو الصحافة، أو من حق الناس في الاجتماع سلمياً، وفي مطالبة الحكومة بإنصافهم من الإجحاف".

نتيجةً لذلك، ليس من السهل دائماً معرفة الغاية من التعديل الأول. وبهدف مساعدتي على فرز الأجمات القانونية، جلستُ مع العالِم الشهير في التعديل الأول، لي بولينغر، وهو أيضاً رئيس جامعة كولومبيا. "يمكن وصف نظرية التعديل الأول بالذُّهان الارتيابـي"، قال بولينغر. اعتقد المؤسسون أن الديموقراطية تتطلب حرّية انتقاد الحكومة. بالنتيجة، إن الاختبار الهام لأية قضية قانونية مرتبطة بالتعديل الأول هو: هل النشاط ذات الصلة يحدّ من المشاركة في النقاش الديموقراطي؟

كانت المحكمة العليا حريصة للغاية على كبح أية نشاطات إذا جمّدت تلك التقييدات المشاركة العامة في الديموقراطية. على سبيل المثال، حكمت المحكمة العليا في العام 1964 بأن شركة نيويورك تايمز غير مُلزَمة بنشر إعلان يتضمن أكاذيب عن موظف عام لأن "الإرغام على انتقاد سلوك موظف ما لضمان حقيقة كل تأكيداته الواقعية... يؤدي إلى رَقابة ذاتية مشابهة". وفي العام 2000، حكمت المحكمة العليا بأن الجمعية الكشفية الأميركية للفتيان غير مُلزَمة بقبول شخص غير سوي جنسياً في عضويتها لأن إرغام المجموعات على قبول أعضاء ينتهك حرّية إقامة الصِّلات المعبِّرة. "يحمي التعديل الأول التعبير، سواءً عن الاختلاف الشعبـي أم لا"، كتب رئيس المحكمة العليا وليام ه. رينكويست.

ولكن المحكمة العليا لم تكن متفتحة الذِّهن على النقاش الذي يعتبر الرَّقابة مؤذية لمجتمع حرّ. ففي العام 1972، حكمت المحكمة بخمسة أصوات في مقابل أربعة بأن المواطنين الأميركيين الذين تمّ التجسس عليهم من قِبَل برنامج الرَّقابة التابع للجيش الأميركي لا يمكنهم أن يُثبتوا تعرّضهم لأي ضرر، ولذلك "لا مصلحة شخصية لهم في ما سيؤول إليه النقاش" لأجل الإنصاف القضائي. وفي العام 2013 أيضاً، حكمت المحكمة العليا بخمسة أصوات في مقابل أربعة بأن المواطنين الأميركيين الذين تم التجسس عليهم من خلال برنامج التنصت التي تُديره وكالة الأمن القومي، دون الحصول على مذكرة، لا يمكنهم أن يُثبتوا تعرّضهم لضرر "حسّي، محدَّد وفعليّ، أو وشيك" يتطلب عملاً قضائياً.

من جهة ثانية، صُدمتُ ببلاغة معارَضة رئيسَي المحكمة العليا وليام أو. دوغلاس وثورغود مارشال في قضية العام 1972. لقد دعيا برنامج رَقابة الجيش الأميركي "سرَطاناً في الجسم السياسي" الذي "يخوض حرباً مع مبادئ التعديل الأول". لقد كتبا: "عندما ينظر موظف استخبارات من فوق كتف كل مُخالف لنمط الجماعة في المكتبة، أو يسير بجانبه وبشكل غير مرئيّ في صفّ محرِّضين على الإضراب، أو يتسلل إلى ناديه، لا تعود تُرى أميركا، التي امتُدحت ذات مرة بأنها صوت الحرّية في أنحاء العالم، في الصورة التي وضعها جيفرسون وماديسون بل في الصورة الروسية".

á á á

بعد مناوشتهما مع الأف بـي آي، بات ياسر وخالد يرتابان بكل سيارة تمرّ بجانبهما. ولكن الخوف زال ببطء وحلّ مكانه شعور جديد: تقبُّل كونهما مراقَبَين.

"ماذا يمكنك أن تفعلي؟" قال لي خالد عندما التقينا في ستاربوكس في سانتا كلارا، بعد عام من الحادث. "نحن على وشك فقدان كل خصوصيتنا بأية حال. لقد أخذتها التكنولوجيا منا".

أطلعني خالد على ما حدث بعد ظهور الأف بـي آي عند باب ياسر: بعد أيام قليلة، اتصلت عميلة الأف بـي آي، جنيفر، بالهاتف خالد المحمول وتركت رسالة. لم يُعِد الاتصال بها. ومذاك الحين، قال، غالباً ما يتلقى اتصالات هاتفية من رقم محجوب - عندما يُجيب على الاتصال يسمع رنيناً ليس إلا. "سيتصلون بـي مرتَين في اليوم لمدة يومَين، ومن ثم ينقطعون عن الاتصال لمدة ثلاثة اسابيع"، قال لي.

مبدئياً، كان ينظر تحت سيارته كلما دخلها، ولكنه كفّ عن القيام بذلك بعد فترة. لقد تصوّر أن الأف بـي آي ستجد طريقة لملاحقته إذا رغبت في ذلك.

لقد تراجعت مشاركته على Reddit وباتت تتقاطر ببطء. واستبدل مقالاته الطويلة عن الظلم بتعليقات قصيرة في الغالب غير مثيرة للجدل.

وكفّ خالد أيضاً عن التسكع مع ياسر. وعندما بدأ مستخدمو Reddit الإلحاح على خالد لتزويدهم بمعلومات عن قضية التعقُّب بواسطة نظام تحديد المواقع العالمي، كتب خالد، "أصبح بمثابة نَضحاً قشارياً علينا نوعاً ما، لذلك انهرنا نوعاً ما".

عندما التقيتُ خالد، كان قد عاد للتوّ من زيارة إلى مصر، وقال لي إنه يفكر في الانتقال إلى هناك. قال إن الناس في الولايات المتحدة قانعون برؤية حقوقهم تنـزلق بعيداً.

"هنا وهم الحرّية"، قال. "هناك الحرّية الفعلية. يمكنك القيام بما يحلو لك".

á á á

وجدت صعوبة في القول لخالد إنه يُفترض به أن يكون أكثر تفاؤلاً حيال حرّيته. لسوء الحظ، غالباً ما عومل المسلمون في أميركا كمشتبَه بهم في صف لتمييز الوجوه في مراكز الشرطة منذ هجوم القاعدة على أميركا في 11 أيلول/سبتمبر 2001.

بعد 11/9، أعدّت الأف بـي آي نظاماً لإدارة النطاق بهدف تحليل مكان إقامة المسلمين، مستعينين ببيانات تجارية، واستهداف تلك المجموعات التي تحتوي على مُخبِرين. من غير المفاجئ أن يترافق هذا الأمر مع زيادة في حالات الادعاء على المسلمين في قضايا إرهابية. لقد تفحّص الصحافي

الاستقصائي تريفور أرونسون الدعوات القضائية الـ508 التي تقدّمت بها الأف بـي آي منذ 11/9 ووجد أن مُخبرين استُخدموا في نحو نصف الحالات، واستُخدم رجال شرطة متخفّين في ثلث الحالات. جاء في تقرير أرونسون أن المُخبِرين يستهدفون أشخاصاً يائسين، غير منيعين، في غالب الأحيان، ويُغوونهم للوقوع في شرك مكيدة إرهابية مزيَّفة. "لم يسبق أن استُخدم رجال شرطة متخفّون للإيقاع بأشخاص يملكون أسلحة"، قال أرونسون. "في كل الحالات عموماً، توفر الأف بـي آي كل الوسائل المطلوبة".

بُذلت الجهود الأكثر عدائية للتجسس على المسلمين في مدينة نيويورك، من خلال تعاون سرّي بين قسم شرطة نيويورك ووكالة الاستخبارات المركزية (CIA) للتسلل إلى داخل مجموعات سياسية مسلمة، وأحياء، ومناسبات، ومجموعات طلابية، في نيويورك ونيوجرسي. في العام 2008، رافق عميل متخفٍّ مجموعة طلاب مسلمة من سيتي كوليدج في نيويورك في رحلة على متن طَوف في مياه مُزبِدة. عام 2009، أعدّ ضباط متخفّون من قسم شرطة نيويورك منـزلاً آمناً قرب جامعة روتجرز في نيوجرسي، ولكن كُشف النقاب عن تخفّيهم عندما اشتبه المُشرف على المبنى بأنهم خليّة إرهابية، واتصل بالشرطة.

تأمّلوا بقصة أسد دانديا، وهو طالب في مدينة نيويورك، في الحادي والعشرين من العمر، وكان يقوم مُخبِر من قسم شرطة نيويورك بمراقبته. شارك دانديا في تأسيس جمعية خيرية تدعى خدمات نيويورك في سبيل الله، وقد جمعت مالاً لإطعام مشرَّدين ومُعدَمين. وفي آذار/مارس 2012، اتصل به رجل عبر فيسبوك يدعى شاميور رحمَن، وقال إنه يريد الانخراط في نشاطات الجمعية الخيرية. "كان لدينا عدة أصدقاء مشترَكين، وسُررت بمساعدته في بحثه عن تحسين الذات دينياً، لذلك عرّفتُه بأصدقائي في الجمعية"، كتب دانديا في مدوَّنة تصف الرَّقابة التي كانت تستهدفه.

أصبح رحمن ودانديا، وهما في السنّ نفسها تقريباً، صديقَين مقرَّبَين. وزار رحمن منـزل والدَي دانديا عدة مرات، وقضى الليل هناك ذات مرة. كان رحمن فُضولياً أيضاً. "يسأل رحمن كل من يلتقيه عن رقم هاتفه، وبعد دقائق من لقائهم في غالب الأحيان"، كتب دانديا. "وكان يحاول في غالب الأحيان أيضاً التقاط صور لأشخاص - أو معهم - التقاهم من خلالي".

في 2 تشرين الأول/أكتوبر 2012، نشر رحمن رسالة على فيسبوك تكشف أنه كان مُخبِراً في قسم شرطة نيويورك. وأخبر الصحافة في وقت

لاحق بأنه أصبح مُخبِراً بعد سلسلة من الاعتقالات طالت قاصرين يتعاطون الماريجوانا، وأنه كان يتقاضى 1,000 دولار في الشهر. ولكن رحمن تعب أخيراً من التجسس على أصدقائه وتخلّى عن عمله. "لقد كرهتُ استغلال الناس بهدف جَني المال"، قال رحمن للأسوشيتد بريس. "ارتكبت خطأ".

صدم تصريح رحمن أصدقاءه. "عندما سمعتُ الخبر، تسمّرت في مكاني"، كتب دانديا في مدوّنته. "كان شعوراً مروِّعاً. لم أصدّق أن مُخبِراً في قسم شرطة نيويورك كان في منـزلي". لقد ألقى الحادث بظلاله أيضاً على جمعية دانديا الخيرية التي أُعيد إطلاق اسم مسلمون في خلوة مع أنفسهم عليها. وطلب المسجد المحلّي من دانديا الكفّ عن عقد لقاءات خيرية في المسجد، والإقلاع عن جمع تبرعات من المجتمعين. عانت الجمعية الخيرية مالياً ومعنوياً، يقول دانديا. وشرع دانديا وأعضاء آخرون بجعل وجوههم مُبهَمة في صور ينشرونها في صفحة الجمعية على فيسبوك. لقد اشترك دانديا في دعوى قضائية ضد قسم شرطة نيويورك.

"اعتدتُ محاولة أن أكون شاملاً وعامّاً بأكبر قدْر ممكن في شأن العمل الخيري - الآن، أتواصل بشكل رئيسي مع أشخاص تربطني بهم معرفة شخصية"، كتب دانديا.

á á á

انسحب ياسر عفيفي أيضاً إلى ما وراء دِرعٍ واقٍ. لم يَعُد يتسكع مع صديق الطفولة، خالد. هو منشغل في عمله كبائع برامج كمبيوترية، ويحضر دروساً ليلية للحصول على شهادة من الكلّية. لقد ادّخر مالاً لشراء منـزل، وزوجته حامل.

"إذا نضجتُ ولم ينضج صديقي المفضل، يصعب التسكع معه"، قال لي. "في هذه المرحلة من حياتي، إن تسكّعي معه هو تضييع تام لوقتي".

لا يستطيع ياسر تحمّل تبِعات المجازفة. هو يعتقد بأنه ما يزال على قائمة مراقبة من نوع ما. فعندما عاد وزوجته من رحلة إلى بويرتو فالارتا، المكسيك، عام 2012، تمّ استجوابه لنحو ساعة لدى وصوله، في حين فتش عملاء فيدراليون حقائبه وطرحوا أسئلة. قال إن العملاء أخذوا هاتف زوجته، ولكنه رفض إعطاءهم هاتفه. "كانوا يطرحون أسئلة لا يحق لهم طرحها. لقد سألوا زوجتي عن سبب انفصالها عن زوجها السابق"، قال لي. "لقد شعرتُ بغضب شديد".

ولكنه يحاول التحكم بغضبه. "هل أرغب في سياسة معيَّنة يوقفون من خلالها مضايقة الأميركيين المسلمين؟ أجل"، قال لي أثناء وقوفنا في المكان

حيث أوقفته الأف بـي آي. "هل أرغب في أن يكتبوا لي اعتذاراً بسبب وضع [نظام تحديد المواقع العالمي المتعقّب] على سيارتي؟ أجل. ولكنها أمور لا أعتمد عليها. أنا أواصل حياتي. أريد أن أكون ثرياً. أريد أن تكون لي عائلة. أريد الحلم الأميركي. أريد أن يحصل عليه آخرون أيضاً".

بعد عام من تلك المحادثة، حقق ياسر حلمه. لقد اشترى وزوجته منـزلاً في جنوب سان خوسيه. وذات يوم حارّ، جئت لزيارتهما في شارعهما غير النافذ بواسطة سيارتي المستأجَرة. فركنتُ بجانب بركة السباحة الصغيرة التي تتشاطرها كل المنازل في المجمَّع السكني.

في الداخل، أراني ياسر أريكة جلدية قشيبة في غرفة الجلوس، وأغطية الأسرّة والستائر الملوَّنة في غرفة نوم ابنتهما. كانت هناك مِشواة مشبكية في الفناء الجانبـي الصغير.

أثناء قيامي بجولة على المنـزل، واصلتُ التفكير في أنسبائي الذين هاجروا من روسيا إلى الولايات المتحدة عند منقلَب القرن العشرين. كانوا يفرّون من عالَم حيث اليهود مضطهَدون بسبب معتقداتهم. لقد عانوا الأمرَّين للقدوم إلى هنا - كانت والدة جدي تعمل في متجر سكاكر، ووالد جدي بائعاً متجولاً - ولكن الأمر جدير بالمحاولة لأجل الحرّية.

جاءت عائلة ياسر من مصر إلى هنا بحثاً عن فرصة اقتصادية. عمل ياسر بكدّ وحقق نجاحاً مالياً هنا، ولكنه لم ينعم بالحرّية التي وُعد بها؛ بدلاً من ذلك، أخضع نفسه للرَّقابة وقمع صِلاته.

يتمتع ياسر بحرّية شراء مشاوٍ مشبكية، ومنازل في المدينة، وأريكات جِلدية بالدَّين، ولكن ليس حرّية إقامة الصِّلات بأشخاص يُطلقون دُعابات عن الحظر التي تفرضة الحكومة في المطارات على مزيل الرائحة.

الفصل الخامس

رفع مستوى الأمن الكمبيوتري إلى الدرجة الفُضلى

في عالم حيث كل شيء تقريباً مراقَب، يسهل الشعور بأن الخصوصية هي أمر ميؤوس منه. في غالب الأحيان، عندما أخبر الأشخاص الذين ألتقيهم للتوّ بأنني أكتب عن الخصوصية، يكون جوابهم الفوري، "لقد استسلمتُ. لم يَعُد هناك خصوصية".

في الحقيقة، لقد فكرت في الاستسلام أيضاً. فطوال ثلاث سنوات، كتبت عن اجتياحات الخصوصية التي جعلت منها التكنولوجيا أمراً ممكناً. ولكنني

لم أفعل الكثير كي أحمي نفسي. كنت أقول إن انشغالي الكبير هو السبب، ولكنني كنت مغمورة في الواقع باستحالة فعل أي شيء.

بعد العديد من المحادثات، بدأت أشعر بالذَّنْب. هل إن تطرّقي إلى اجتياحات الخصوصية يسهم في الواقع في شعوري بأن الخصوصية أمر ميؤوس منه؟

أنا متفائلة بطبيعتي: أردت الاعتقاد بوجود أمل. وأنا معارِضة بالمَولد: أردت دَحض المتشككين. وأخيراً، أنا عنيدة: عزمتُ على العثور على بعض الأمل.

لذلك قررت محاولة تجنّب شبكات التعقُّب، بالرغم من احتمال عدم تمكّني من ذلك. سأحاول تجنّب تعرّضي للمراقبة أثناء قيامي بنشاطاتي اليومية كالقراءة والتسوّق. سأُخفي مكان وجودي - في المنـزل وخارجه. سأُحكم إغلاق رسائلي ونصوصي الموجَّهة عبر البريد الإلكتروني بواسطة المُرادف الرقمي للشمع الساخن. سأجد طرقاً لأقيم صِلات بأشخاص وأفكار بحرّية. سأحاول إيجاد طريقة لحماية أطفالي من بناء أثر رقمي يتعقّبهم ويلازمهم طوال حياتهم.

كانت مهمة مُرعِبة. "لا يمكنني القيام بذلك"، قلت لصديقة مقرَّبة. "كيف أعيش بدون بطاقة ائتمان؟ بدون هاتف محمول؟ سيكون ذلك أمراً غير مسؤول برأي ابني وابنتي".

ولكنني أدركت أن أسئلتي هي ما أحتاج إلى تفحّصها بالتحديد: هل يمكن العيش في العالم الحديث وتجنّب شبكات التعقُّب؟ هل وافقتُ بطريقة ما على الرَّقابة الكلّية الوجود - مقايضةً بياناتي بخدماتٍ أو أمان مجّاني - كما يؤكد العاملون في ميدان الرَّقابة؟ ماذا يحدث إذا حاولت سحب موافقتي؟

á á á

كانت خطوتي الأولى تحديد التهديدات المحيطة بخصوصيتي.

في صناعة الأمن الكمبيوتري، إن تحديد هوية أخصامكم يُدعى رفعاً لمستوى أمنكم الكمبيوتري إلى الدرجة الفُضلى. تتمثل الفكرة بقدرتكم على حماية أنفسكم ضد التهديدات المعروفة فقط. ويدعو الخبير في صناعة الأمن الكمبيوتري، بروس شنير، هذا الأمر الدرسَ الأول عن الأمن: الأمن هو تنازل عن ميزةٍ للحصول على أخرى. "لا وجود للأمن المُطلَق"، كتب في مقدمة كتابه شنير والأمن . "تقتضي الحياةُ المخاطرةَ، ويستلزم الأمنُ المُطلَق تنازلاً عن ميزات للحصول على أخرى. نحصل على الأمن في مقابل التخلّي عن

شيء ما: مال، وقت، ملاءمة، قدرات، حرّيات، ألخ". ما تتخلوا عنه يعتمد على ما تحاولون حمايته ومن تحاولون حمايته منه.

قد يكون التركيز على الخصم غير المناسب كارثياً. تأمّلوا بمسألة ديفيد بتريوس، المدير السابق لوكالة الاستخبارات المركزية.

في العام 2012، كشفت الأف بـي آي النقاب عن الجنرال بتريوس الذي كان يستخدم تقنية غير متطورة أثناء انخراطه بعلاقة غرامية خارج الزواج مع واضعة سيرة حياته، بولا برودويل. لقد ندّد به المنتقدون بسبب استخدامه حساباً مشتركاً على بريد غوغل الإلكتروني، وقد ترك وبرودويل فيه مسوَّدة رسائل لأحدهما الآخر - دعت مجلة فورين بوليسي هذا الأمر "مهارة تجسسية قديمة". ولكن المشكلة الحقيقية تمثلت بأن الجنرال أساء تقدير خصمه.

كان وعشيقته يحاولان إخفاء علاقتهما الغرامية عن الشريك - الزوج أو الزوجة. في تلك الحالة، يُعتبر حساب مشترك على بريد غوغل الإلكتروني يمكن ولوجه من أجهزة كمبيوتر غير موجودة في منـزلَيهما، حمايةً كافية. ولكنهما لم يتصوّرا أن الأف بـي آي ستشرع باستجواب برودويل بسبب توجيه رسائل تهديدية عبر البريد الإلكتروني لمصمِّمة مناسبات متطوِّعة في تامبا، فلوريدا، تدعى جيل كيلي. وحصلت الأف بـي آي على عناوين بروتوكول الإنترنت التي وُجّهت من خلالها رسائل البريد الإلكتروني، وذلك عبر استدعاء للمثول أمام المحكمة، على الأرجح، وُجِّه لمن يزوّد برودويل بالبريد الإلكتروني. اقتفى عملاء الأف بـي آي عناوين البروتوكول تلك وصولاً إلى مجموعة منوّعة من شبكات واي - فاي، بما في ذلك عدة فنادق، ومن ثم ولجوا قوائم بنـزلاء الفنادق بحثاً عن تواريخ توجيه رسائل البريد الإلكتروني. وسرعان ما وجدت الأف بـي آي أن بولا برودويل كانت نـزيلة مشترَكة في تلك الفنادق في تلك التواريخ. ومن هناك، بحثوا في بريد برودويل الإلكتروني إما عبر مذكرة تفتيش أو عبر استدعاءات للمثول أمام المحكمة - واكتشفوا علاقتها ببتريوس.

فلو أراد الجنرال وعشيقته أن يفوقوا الأف بـي آي براعة لَقاما على الأقل بخطوات معيَّنة لإخفاء عناوين بروتوكول الإنترنت التي ولجا عبرها حسابَيهما، واستخدما التشفير، وحرصا على أن يضعا حسابَيهما بأسماء زائفة. حتى في هذه الحالة، لا شيء يضمن عدم الكشف عن هويّتهما.

بالرغم من كل شيء، إن الخصوصية المثالية غير ممكنة حتى ولو حدّدتم هوية خصمكم بشكل صحيح.

تأملوا بحالة أخرى: تيودور جيه. كاتشينسكي، المسؤول الوحيد عن عمليات تفجير متعددة بالبريد الإلكتروني. طوال عقد من الزمن، عاش كاتشينسكي كناسك في كوخ من غرفة واحدة - بدون كهرباء، أدوات صرف صحي، أو هاتف - في منطقة نائية من مونتانا أثناء قيامه بسلسلة من التفجيرات عبر البريد الإلكتروني أودت بحياة ثلاثة أشخاص وأصابت اثنَين وعشرين بجراح. حتى إن الناسك لم يتمكن من الإفلات من الأف بـي آي التي اقتفت أثره إلى كوخه في النهاية، ويعود سبب ذلك في المقام الأول إلى قيام شقيقه بتقديم بحث وضعه كاتشينسكي عندما كان شاباً، فتمّت مقارنته مع تحليل لُغوي لخط يده الحالي.

وهو أمر جيد: كان المجتمع أفضل حالاً عندما ألقت الأف بـي آي القبض على كاتشينسكي وأنهت مَرحه التفجيري. ولكن بقيّتنا سيكونون أفضل حالاً عندما نرفع مستوى الأمن الكمبيوتري الخاص بنا إلى الدرجة الفُضلى.

á á á

ماذا يعني لي رفع مستوى أمني الكمبيوتري إلى الدرجة الفُضلى؟

أنا صحافية مع ابن في مرحلة ما قبل المدرسة وابنة في المدرسة الابتدائية. زوجي أستاذ جامعي يسافر إلى الخارج في غالب الأحيان لأجل بحثه.

إذا أردت وصف عائلتي بكلمة بسيطة واحدة فستكون "ناشطة". نحن نسير على الدوام في اتجاهات عديدة مختلفة. والخصوصية والأمن هما من الأمور التي تُغفلونها عندما تكونون في عَجَلة من أمركم.

ومع ذلك، أريد حماية نفسي وصغيرَيّ من التعقّب غير المميِّز. أريد أن نحظى بحرّية الاشتراك مع أشخاص وأماكن وأفكار دون القلق من إمكانية تقييد تلك الاشتراكات لفُرصنا المستقبلية.

أريد أيضاً حماية نفسي من التهديدات التي تستهدف صحافيين. بالرغم من كل شيء، كانت إدارة أوباما عدوانية للغاية في مقاضاة الأشخاص الذين يمررون معلومات حساسة للصحافيين. فمنذ العام 2009، قاضت الإدارة ثمانية مسرِّبين حكوميين لمعلومات سرّية بتهمة انتهاك قانون التجسس الذي استُخدم ثلاث مرات فقط في السنوات الاثنتَين والتسعين الماضية ضد موظفين حكوميين بسبب تزويد صحافيين بمعلومات سرّية.

وقلقي على نفسي أقل لأن الأمر لا ينتهي بالصحافيين في السجن في غالب الأحيان، كما يبدو. لسوء الحظ، إن الذين يسرّبون معلومات لصحافيين هم من ينتهي بهم الأمر في السجن. أريد أن أكون قادرة على

منح مصادري تعهّداً بالسرّية يمكنني الإيفاء به.

إذاً، لديّ تهديدان في الواقع: تعقُّب غير مميِّز وهجمات تستهدف صحافيين ومصادرهم.

á á á

أثناء رفع مستوى الأمن الكمبيوتري إلى الدرجة الفُضلى، من الهام أيضاً تقييم مكامن القوة والضعف لديكم.

يتمثل مكمن قوتي بكتابتي عن الخصوصية والتكنولوجيا طوال سنوات، لذلك يمكنني الاتصال بعدد كبير من الخبراء طلَباً للمساعدة والتوجيه. أنا محظوظة أيضاً بسبب عدم وجود مسائل متعلقة بالخصوصية يتعيّن عليّ "ترتيبها". فمنذ سنوات قليلة، عندما نُشر كتابـي عن الشبكة الاجتماعية ماي سبايس، عملتُ لتكون سمعتي على شبكة الإنترنت صامدة للرصاص. لقد تشاورتُ مع مستشارين في مجال إيصال محرك البحث إلى الدرجة الفضلى ليساعدوني على بناء موقع على الويب وجعْل نِبذات شبكتي الاجتماعية سليمة كي تطغى على نتائج البحث عني على غوغل مواضيعٌ كتبتها عن نفسي، لا مواضيع كتبها آخرون عني.

كذلك، فابني وابنتي صغيران وبياناتهما غير متوافرة بعد بشكل علَني. فهما لا يملكان هواتف محمولة، ولا يلجون أجهزة كمبيوتر. لقد قصرا ولوجهما على الآي باد، ولا حسابات لهما على مواقع التواصل الاجتماعي (باستثناء تلك التي أعدّتها مدرسة ابنتي لها داخل حديقتهم المسيَّجة). لذلك، لا يتعيّن عليّ "ترتيب" كثير من الأمور الخاصة بهما.

ولكن مكامن الضعف لديّ عديدة، وربما يكون افتقاري إلى الصبر أكبرها. فغالباً ما أسلك طُرقات مختصَرة بدلاً من جلوسي القُرفُصاء لاكتشاف سبب عدم فاعلية أدواتي التكنولوجية. نتيجةً لذلك، أكون قابلة لترك نفسي عُرضة للأذى.

وهناك مسألة ضخمة أخرى: عنوان منـزلي غير خافٍ على أحد. عندما اشتريتُ وزوجي منـزلنا ورمّمناه، رضختُ لالتماسات زميلة لي في وول ستريت جورنال ووضعتُ مدوَّنة عن الترميم خاصة بقسم العقارات في الصحيفة الذي يُنشَر عبر شبكة الإنترنت. وبالرغم من عدم قيامي أبداً بنشر العنوان الصحيح لمنـزلنا، فقد عرفته مدوَّنة واحدة على الأقل من الصور الفوتوغرافية. لذلك، زالت كتلة واحدة أساسية لبناء الخصوصية.

ولا يأبه زوجي أيضاً بالخصوصية. فهو أستاذ جامعي ويُطلق على الدوام دُعابات عن أن قرّاء مقالاته سيتضاعف إذا اقتحم شخص ما ملفاته.

فهو لا يأبه بالخصوصية فحسب، بل إن ميدان عمله ينتهك حُرمة الخصوصية. هو مهندس ميكانيكي، وأحد مشاريعه تثبيت أجهزة تحسّس بُعدية لمراقبة استخدام الطاقة. في الواقع، لقد ثبّت أجهزة تحسّس في منـزلنا دون أن يتكبّد عناء سؤالي عن الأمر. لقد اكتشفتُ الأمر يوم انتقالنا إلى المنـزل حيث كان أحد طلابه المتخرّجين يُتِمّ عملية مدّ أسلاك النظام.

فمراقيب الطاقة الفورية التي ثبّتها ممتازة نوعاً ما - يمكننا رؤية الطاقة التي نستخدمها في أي وقت، ويمكننا التعلّم من أنماط استخدامنا لها. بالطبع، من الغريب إلى حد ما أن يقوم طلابه المتخرّجون بمراقبة استخدامنا للطاقة.

"ماذا تفعلون أيام الجمعة؟" سأله أحد طلابه ذات يوم. "يرتفع استخدامكم للطاقة أيام الجمعة". لقد تبيّن أن عاملة التنظيف تأتي أيام الجمعة وتشغّل المكنسة الكهربائية.

لا يأبه صغيراي أيضاً بالخصوصية. بالنسبة إليهم، "الخصوصية" مجرد كلمة تعني "لا". فالخصوصية هي سبب عدم تمكنهما من نشر أفلام فيديو على اليوتيوب. والخصوصية هي سبب عدم سماحي لهما بالانتساب إلى شبكات التواصل الاجتماعي الخاصة بالأطفال. والخصوصية هي سبب شكواي لمعلّماتهما بسبب نشر صور لهما على مدوَّنة لا تحميها كلمة مرور.

في الواقع، تعتقد ابنتي أن الخصوصية أمر يجب إلغاؤه. هي تستمتع بمحاولة معرفة كلمات مروري. ذات مرة، اكتشفت كلمة مروري على جهاز الآي فون الخاص بـي، وولجتْ هاتفي، وبدّلتْ كلمة المرور، ومن ثم نسيتْ الكلمة الجديدة، تاركةً إيّاي غير قادرة على ولوجه، ومُرغِمةً إيّاي على إزالة كل المعلومات المخزَّنة في الجهاز لإعادته إلى حالته الأصلية كي أتمكن من ولوجه.

لذلك، سأخوض هذه المعركة بمفردي، أقلّه على جبهة المنـزل، وسيكون زملائي الجنود شبكةً متداعية من التكنولوجيين، ومتسللين إلى ملفات كمبيوترية، ومواطنين قلِقين في مختلف أنحاء العالم.

á á á

أنا بحاجة الآن إلى خطة قتالية للدفاع عن نفسي، وإلى تحديد المدى الذي سأبلغه في هذه المواجهة: هل سأعيش في ملجأ حصين؟ هل سأغيّر اسمي؟

لقد قرأت كتباً قليلة عن حماية الخصوصية، وكانت متطرفة على نحوٍ

مُجفِل. في كيف تكونون غير مرئيين: احموا منـزلكم، أطفالكم، أصولكم، وحياتكم ، يقول جيه. جيه. لونا إن "رحلتكم إلى الخفاء يجب أن تبدأ بالخطوة الأولى: فصل اسمكم عن عنوان منـزلكم". وإذا كان عنوانكم معروفاً علَناً، ينصح بالانتقال.

يقترح لونا إنشاء شركة محدودة المسؤولية في نيو مكسيكو تملك أصولكم - منـزل، سيارة، وهكذا دواليك. ويبلغ حد اقتراح عدم تمكنكم من إرسال أبنائكم إلى مدارس عامة لأنها تكشف عن عنوانكم. "هناك علاجان فقط لهذا الخطر"، يكتب. "إما وفّروا لأبنائكم تعليماً منـزلياً أو ضعوهم في مدرسة خاصة مستعدة لضمان خصوصيّتهم".

لا أستطيع تحمّل كلفة وضع صغيرَيّ في مدرسة خاصة أو الاستقالة من وظيفتي لتوفير تعليمٍ منـزليّ لهما، كما أنني لا أريد السعي وراء أيٍّ من الخيارَين.

رفع مستوى خصوصية لونا على الإنترنت إلى الدرجة الفُضلى؟ محقِّقون خاصون. حتى وإن عملتم بنصيحته، يقول، بإمكان محقِّق خاص تتوافر له مخصصات مالية غير محدودة العثور عليكم في نهاية المطاف.

في أمّة تحت الرَّقابة ، يقول بوسكن تي. بارتي، وهو الاسم المستعار لكينيث دبليو. رويس، إن "القانون لم يَعُد صالحاً لأن أميركا بدّلت اتجاه محورها القانوني". وينصح القراء باختزان أسلحتهم، وزراعة طعامهم الخاص، وتوفير تعليم منـزلي لأبنائهم، وتشغيل جهازهم الكمبيوتري بواسطة قرص صلب يحتوي على نظام تشغيل يدعى بابـي لينوكس (Linux Puppy).

هو يرى في رفع مستوى أمني الكمبيوتري إلى الدرجة الفُضلى حكومةً عدائية مستعدة للانقضاض على المدنيين.

لستُ مصابة بذلك الذُّهان الارتيابـي بعد. لا أعتقد أن الحكومة قضية خاسرة. ما أزال أؤمن بالنظام القانوني وبأن نظام الضوابط والتوازنات الخاص بنا صالح في الغالب. لست مستعدة للشروع باختزان أسلحة وزراعة طعامي (باستثناء قليل من البندورة والرَّيحان في الفناء الخلفي كل صيف). ولا أخطط للشروع بتوفير تعليم منـزلي لصغيرَيّ، أو بالانتقال إلى اقتصاد الدَّفع نَقداً.

أحاول الدفاع عن نفسي من تهديد مختلف: نشوء تعقُّب غير مميِّز - شبكات التعقُّب التي تهدف إلى وضع كل عنصر من حياتنا في سجلّ دائم. أنا قلِقة من أن يمنعني هذا التعقُّب المميِّز من الاشتراك مع أفكار وأشخاص معيَّنين، ومن التسبب بمعاناة اقتصادية، ومن إنشاء ثقافة خوف.

أنا قلِقة، في أسوأ الحالات، من أن يؤدّي التعقُّب المميِّز إلى إنشاء دولة رَقابة توتاليتارية.

á á á

لرفع مستوى أمني الكمبيوتري إلى الدرجة الفُضلى، استشرت خبراء من كل الأنواع - بدءاً بموظفين حكوميين عالِي المستوى مزوَّدين بتصاريح أمنية للتعاطي مع متسللين إلى ملفات كمبيوترية يضعون أدوات مضادة للرَّقابة. فلكل منهم اقتراح مختلف. على سبيل المثال، نصحني بعضهم باستخدام أجهزة كمبيوتر مختلفة لغايات مختلفة - واحد للعمل المصرفي، واحد للعمل الشخصي، وواحد للعمل المهني؛ ونصحني آخرون باستخدام برنامج كمبيوتري يقسم جهاز كمبيوتر واحد إلى ثلاثة أقسام منفصلة، محاكياً عملية إعداد ثلاثة أجهزة كمبيوتر؛ وقال آخرون إن لا فائدة من محاولة تقسيم الجهاز لأن الأمر سينتهي ببياناتي ممزوجة بأية حال. وبعد العديد من هذه المحادثات، أدركتُ أن لا وجود لرصاصة فضّية.

لقد تعيّن عليّ وضع خطتي القتالية. فأنشأتُ برنامج جداول بيانات، موجِزةً التهديدات وتكتيكاتي المقترَحة لمواجهة أي خطر. ستكون مواجهة بعض التهديدات سهلة نسبياً على الأرجح؛ لتجنّب التعقُّب الإعلاني عبر الإنترنت، سأستخدم أنواعاً مختلفة من البرامج المضادة للتعقُّب وأقيّم البرنامج الأفضل. ولكن تهديدات أخرى كانت أكثر تعقيداً؛ لم أكن أملك تكتيكاً جيداً لمواجهة قارئات لوحات التسجيل المؤتمَتة التي تصوّر لوحة سيارتي عندما أمرّ أمامها. لقد اقترح أحد الخبراء تغطية لوحة تسجيل سيارتي برَذاذ أو بلوح زجاج يُحبط عمل الكاميرات العاملة بالأشعة ما دون الحمراء. ولكن في نيويورك حيث أعيش، من غير القانوني تغطية لوحة تسجيل بطريقة "تشوّه صورة فوتوغرافية أو مسجَّلة لهذه اللوحات".

أدركتُ أنني بحاجة إلى تطوير بعض التوجيهات، قبل اختيار تكتيكاتي، للسيطرة على سلوكي. لذلك، طوّرت قواعد الاشتباك الخاصة بـي.

لا أخرق القانون . لا أحاول التهرّب من الضرائب أو خرق القانون. لذلك، سأقوم بأعمال قانونية فقط. يعني ذلك عدم حجب لوحة تسجيل سيارتي.

أحياناً، لا يكون ما هو قانونيّ واضحاً. تأمّلوا برخص السَّوق الزائفة. لقد طلبتُ من مارك إيكنويلر، وهو محامي رَقابة سابق في وزارة العدل الأميركية، النُّصح حول ما إذا كانت الهوية الزائفة قانونية.

فلفت مارك نظري إلى التشريع الذي يجعل من استخدام هويّة

شخص آخر بهدف ارتكاب جريمة أمراً غير قانوني. ولكنه لفت نظري أيضاً إلى حكم صادر عن المحكمة العليا عام 2009 فسّر بأن التشريع يوجب إبلاغ المخالف بأنه أساء استعمال الأوراق الثبوتية لشخص فعليّ. قد يشير ذلك ضمناً إلى أن استخدام رخصة سَوق زائفة تابعة لشخص غير حقيقي هو أمر مقبول. ولكنه لفت نظري عندئذٍ إلى تشريعَي الاحتيال البريدي والاحتيال الهاتفي الإلكتروني اللذَين ينصّان على عدم قانونية الانخراط في "أية خطة" للحصول على مال أو مِلكية من خلال "وعود زائفة أو احتيالية".

من غير المفاجئ رفض مارك تقديم نُصحٍ رسمي لي حول الحصول على هويّة زائفة أم لا. من جهة ثانية، تشير الحالات كما يبدو إلى أنني سأكون آمنه على الأرجح مع هويّة زائفة واسم غير حقيقي إذا لم أستعمله لأي نوع من الاحتيال.

ولكن بالرغم من ذلك، قررت عدم الحصول على هويّة زائفة. أفضّل أن أكون على الجانب الآمن للقانون.

أواصل الحياة في العالم الحديث . لست راغبة في الانقطاع عن التكنولوجيا. أعتقد أن التكنولوجيا مكّنت الناس من إحداث تغييرات عظيمة في العالم. أريد ببساطة الحد من العيوب المؤذية للحياة المُشبَعة بالتكنولوجيا.

نتيجةً لذلك، لن أتمكن من تحقيق خصوصية مثالية. فمع خصم موهوب وعازم، يمكن التحايل على أي إجراء تقريباً. روى لي جون جيه. شتروشز، وهو عميل سابق في الـسي آي أيه ومستشار أمنيّ الآن، قصة عن كيفية استخدامه كي يقتحم مقرّ قيادة كيانٍ ماليّ يحظى بحماية جيدة وبثلاث حلقات من الحرس في الخارج. لقد تسلّل داخل صندوق سيارة موظَّف غير مرتاب.

بصورة مماثلة، يمكن التحايل على معظم الأعمال التي سأقوم بها. على سبيل المثال، إذا استخدمتُ شيفرات لولوج محتويات بريد إلكتروني، يمكن للخصم إنـزال برنامج على جهازي الكمبيوتري يلتقط ضَرَباتي على المفاتيح قبل تشفيرها.

لا يتمثل هدفي بتحقيق فوز مهما كلّف الأمر، بل بإرغام خصمي، ببساطة، على الكدّ في العمل أكثر فأكثر. قد لا أكون قادرة على تجنيب نفسي التعرّض للرَّقابة في الشوارع العامة، ولكن ربما يمكنني إرغام خصمي على مشاهدة شريط تسجيل فيديو طوال ساعات بدلاً من اقتفاء أثر

موقعي ببساطة عبر سلسلة من إحداثيات نظام تحديد المواقع العالمي التي يمكن تحليلها بسهولة.

أستخدم أدوات تقليدية . في كتابه الممتع عن الطعام الصناعي، مُعضلة القارِت ، يُعِدّ مايكل بولان وجبة من خلال الاصطياد والتجميع. هو يقتل حيواناً مقززاً، ويبحث عن فِطر في الغابة، ويقطف كرزاً من شجرة جاره. يدعو الأمر "وجبة مثالية".

يعتمد بعض المستشارين في شؤون التسلل إلى الملفات الكمبيوترية مقارَبةً مماثلة للتحدث عن التكنولوجيا. هم لا يثقون بالأدوات التي يمكنهم إعدادها بأنفسهم، تعديلها، أو تصميمها. هم يتحايلون على البرنامج الكمبيوتري المثبَّت في هواتفهم بهدف تسيير برنامج من اختيارهم، ويشغّلون أجهزتهم الكمبيوترية من أقراص صلبة وليس من نظام تشغيل تقليدي.

ربما تكون الطريقةَ "المُثلى" لحماية بيانات المرء، ولكنه بعيداً عن متناول يدي للأسف. أنا بارعة في أمور التكنولوجيا بما يكفي لإدارة موقعي الخاص على الويب، ولكنني لا أثق بنفسي للبدء بتعديل برنامج هاتفي. كما أنني لا أعتقد أنها المقارَبة الصحيحة. فجمال العصر الحديث في غدوّ هذه التكنولوجيات القوية بسيطة أخيراً بما يكفي ليستمتع الشخص العادي بفوائدها.

وهكذا، وكوني نتيجة منطقية لمبدأي التوجيهي بالعيش في العالم الحديث، سأتجنّب بعض التدابير الأكثر تطرفاً المتّخَذة من قِبَل الجمهور المتسلّل الداعي إلى اصطياد طعامكم الخاص. بدلاً من ذلك، سأستخدم أدوات تقليدية هي في متناول معظم الناس المتمتعين ببعض البراعة في أمور التكنولوجيا. (لن أدّعي أن باستطاعة جدتكم القيام بكل ما سأقوم به. ولكن سيكون بإمكان مراهقيكم القيام به).

هدفي عدم الاحتفاظ بأية بيانات . إن أفضل طريقة لحماية بياناتي ليس وهبها. وأفضل طريقة للقيام بذلك تتمثل باعتماد خدمات لا تخزّن بيانات.

بالطبع، هذه الخدمات نادرة، ولكنها موجودة بالفعل. تأمّلوا بمكتب طبيبتي القائم في ناطحة سحاب وسط مدينة مانهاتن. فعلى غرار معظم المباني النيويوركية بعد 11/9، يطلب البوّاب هويّة الزائرين. ولكن مكتب طبيبتي يريد حماية خصوصية المريض. لذلك، يحدّد مكتب الطبيبة لكل مريض شيفرة تُعطى للبوّاب بدلاً من الهويّة. بهذه الطريقة، يتم استرضاء البوّابين دون تخزين أية بيانات عن المرضى.

أثناء رحلتي، سأسعى للقيام بأعمال مع شركات تخزّن أقلّ قَدْر من البيانات الكافية لإتمام مهامها. في بعض الحالات المحظوظة، لن تكون هناك أية بيانات. وفي حالات أخرى، سيكون هناك أقل قَدْر من البيانات.

أستخدم اختبار بِركة الوحل . تتمثل إحدى الطرق لتحديد ما إذا كنتُ قد خفّضت أثر بياناتي إلى الحد الأدنى باستخدام ما يدعوه بعض مهندسي الأمن "اختبار بِركة الوحل"، ويفسَّر كالتالي: تخيّلوا أنكم أوقعتم جهازكم في بِركة وحل، فانـزلقتم على الوحل، وصدمتم رأسكم لدرجة أنكم نسيتم كلمة المرور لولوج بياناتكم. الآن، هل يمكنكم استعادة بياناتكم من الخدمة التي تعتمدون؟ إذا كان الجواب أجل، تكونون قد تركتم أثراً لبياناتكم. وإذا كان الجواب لا، تكونون قد تجنّبتم بنجاح ترك أثر لبياناتكم. بالطبع، أنتم لا تملكون بياناتكم أيضاً.

تتمثل المشكلة مع اختبار بِركة الوحل بأنكم خاسرون في كلا الحالَين. ولكن هذا الأمر يجعلكم تتذكرون أنكم إذا كنتم تعتمدون خدمة تسمح لكم باستعادة كلمة مروركم المفقود، يمكن للخدمة إذاً ولوج بياناتكم. سأستخدم اختبار بِركة الوحل لتقييم الخدمات التي أعتمدها.

أعمل على تلويث البيانات . عندما لا أستطيع تخفيض أثر بياناتي إلى الحد الأدنى، يمكنني تلويثها باستخدام أسماء زائفة وتوفير معلومات خاطئة.

من المُحرج الإقرار بأنه يصعب عليّ الكذب. فالكذب يضعني في حالة جسدية غير مريحة - حتى ولو كنت أضع اسماً زائفاً في استمارة ويب - أبدأ بالشعور بالحرارة ويشرع نَبَضي بالخفقان بسرعة كبيرة.

ولكن لا شيء أخجل منه في الواقع. حتى الماضي القريب، كانت العمليات التجارية المجهولة الهوية معيار العديد من النشاطات اليومية، فندفع نَقداً، ونتصل من هواتف لا تُظهر هويّة المتصل، ونوجّه رسائل لا تحتوي في غالب الأحيان على عنوان المُرسِل.

لذلك، أتعهّد بتذكير نفسي بأن الأشخاص الذين يطلبون مني ملء استمارات على الإنترنت بهدف إنجاز مهام بسيطة لا يستحقون دائماً إجابات صادقة. إنه طريق صعب على فتاة حاولت أن تكون صالحة ونظيفة بأفضل طريقة إنسانية ممكنة في مدرسة إعدادية لدرجة أنني اعتدت البقاء في الصف أثناء الاستراحات لأنظّف ألواح الطبشور للمدرّسين. ولكنني سأحاول جعل تلويث البيانات جزءاً أساسياً من ترسانة خصوصيتي.

أحمي حركة اتصالاتي . أخطط للعمل بجهد كي أحمي نفسي من تحليل حركة اتصالاتي، أي الناس الذين أتبادل معهم رسائل بريد إلكتروني،

واتصالات هاتفية، ورسائل فورية.

يقلق الناس من اعتراض محتويات بريدهم الإلكتروني، والرسائل النصّية، والرسائل الفورية. ولكن يمكن لتحليل حركة الاتصالات أن تكشف في غالب الأحيان عن محتويات رسالة أو أكثر من مجرد محتويات. فإذا كنت أتبادل ست رسائل في اليوم مع تاجر مخدرات، هل تكونون بحاجة حقاً لمعرفة ما نقول؟ فحجم الرسائل وحده سيوصلني إلى قائمة تجار مخدرات مشتبَه بهم.

وتحليل قوائم اتصالات متبادَلة للعثور على نماذج هي مَهمة تقوم بها أجهزة الكمبيوتر بشكل أفضل من فرز مقادير ضخمة من النصوص. نتيجةً لذلك، سيركّز متعقّبون غير مميِّزين باستمرار على نماذج حركة الاتصالات أولاً. إذاً، سأضع مسألة الدفاع عن نماذج حركة اتصالاتي في أولى أولوياتي.

أستخدم اتصالات فورية . يقتضي قانون التنصت حصول ضباط الشرطة على مذكرة تفتيش استثنائية - الحصول عليها أصعب من الحصول على مذكرة تفتيش عادية - قبل اعتراض اتصالات فورية كالاتصالات الهاتفية، والمسامَرة الفيديوية، والرسائل الفورية داخل الولايات المتحدة.

بعد تخزين تلك الاتصالات، يمكن الحصول على البيانات في غالب الأحيان دون الحاجة إلى مذكرة تفتيش. لذلك، فاستخدام اتصالات حالية وعدم تخزينها هي طريقة جيدة لتجنّب التعرّض للتعقُّب. (ما لم تكونوا مشتبَهاً بكم في الواقع، وحصلت الشرطة على مذكرة تفتيش استثنائية لاعتراض اتصالاتكم الحالية - في هذه الحالة، أتمنى لكم الحظ).

من غير السهل تجنّب تخزين نصوص ورسائل فورية لأنكم لا تستطيعون أن تعرفوا في غالب الأحيان ما إذا كان المتلقي يخزن المعلومات. ولكن، لحسن الحظ، لا تخزَّن معظم النقاشات الصوتية والفيديوية بطريقة افتراضية.

نتيجةً لذلك، ما تزال الاتصالات الهاتفية القديمة الطراز العادية إحدى وسائل الاتصال الأكثر حفاظاً على الخصوصية.

أنثر بيانات في كل مكان . إن الأمر الوحيد الأسوأ من فقدان بطاقة اعتماد هي فقدان محفظة نقودكم بأكملها. بشكل مماثل، إن فقدان بعض البيانات ليس سيّئاً بقَدْر فقدان كل بياناتكم. لذلك، سأسعى لنثر بيانات في كل مكان - بهدف تخفيف ضرر التسريبات المحتَّمة، وخروقات البيانات، والتجسس الحكومي، وغيرها، إلى أدنى حد.

على سبيل المثال، سيكون عليّ اختيار الخدمة التي سأحتفظ بها من

بين الخدمات التي توفّرها غوغل - بريد إلكتروني، بحث، خرائط، وهاتف أندرويد. فنظراً لقيام الحكومة بالتقدم بـ21,389 طلباً لغوغل في النصف الثاني من العام 2012 للحصول على معلومات، من المنطقي إذاً عدم تخزين كل بياناتي القيّمة على أجهزة كمبيوتر تجمع غوغل معلومات عن مستخدميها.

بالطبع، لا سبيل لتجنّب تخزين بعض البيانات في قاعدة بيانات غير منيعة - ما لم أقرر تخزين بياناتي في المنـزل. ولكنني آمل في تمكني من التخفيف من حدة مخاطر الكشف عن بياناتي من خلال نثرها في كل مكان.

أَدفع لقاء الأداء . إن العديد من المتسللين إلى الملفات الكمبيوترية الذين يبنون تكنولوجيا لحماية الخصوصية هم موالون لحركة البرامج الكمبيوترية المجانية/غير المقيَّدة. هم يعتقدون أنه يُفترض بالمستخدمين أن يكونا قادرين على بناء وتعديل البرامج التي يستخدمون كي لا يقعوا في فخ أنظمة لا يتحكمون بها.

نظرياً، لا تحتاج البرامج غير المقيَّدة (نملك حرّية تعديلها مثلاً) لتكون مجانية. ولكن معظم الشركات التي تبتغي الربح تفضّل، في الواقع، عدم جعل شيفرتها عُرضة لعدم الإتقان. وهكذا، ينتهي الأمر بمعظم البرامج القابلة للتعديل مجّانيةً.

وتتمثل النتيجة المشؤومة بذُبول الكثير من هذه البرامج بسبب الإهمال عندما ينتقل المبرمِجون الذين يضعونها مجاناً في وقت فراغهم إلى ممارسة هوايات أخرى بسبب عدم وجود دَفق من المداخيل. لذلك، سأسعى أثناء بحثي عن حماية خصوصيتي إلى دعم مشاريع (من خلال تقديم هِبات أو شراء برامج) تعود على مبرمِجيها بأجور لمعيشتهم، أملاً في استمرار المشروع.

قواعد الشفافية . إن المتسللين إلى الملفات الكمبيوترية الذين يسمحون لي برؤية البيانات التي يملكونها عني هم أقل عدائية من المتسللين الذين لن يسمحوا لي برؤية بياناتي.

الشفافية هي الأمر الأساسي. أشعر بأنني أفضل حالاً حيال تقرير الائتمان الخاص بـي لأنني أملك فرصة مراجعته ومناقشة أية أخطاء أعثر عليها. ولكن معظم الشركات التي تتتبّع تحركاتي لن تُريني البيانات التي تملكها عني. يبدو الأمر جائراً. لذلك، أخطط لاعتماد مقاربة سخيّة مع المتسللين الذين يتمتعون بالشفافية. وسأكون أكثر لطفاً مع المتسللين الذين

يسمحون لي بإلغاء بياناتي، تصحيحها، أو سحبها واصطحابها معي.

الخصوصية ذريعة للاعتراض . أطلب على الدوام تفتيشاً من خلال التربيت بدلاً من المرور عبر ماسحات الأجساد في المطار. فللتربيت طابع احتجاجي: تارةً، تدسّ المتفحّصة يدها عميقاً داخل سِروالي أثناء التربيت تحت نطاق الخصر؛ وطَوراً، تسحب المتفحّصة نطاق خصري من الوراء بقوة لدرجة أنني أكاد أقع. بطرق شتّى، التربيت أكثر احتياجاً من الماسحات المؤتمَتة.

ولكن غايتي من عدم اختيار الماسحة تسجيلُ اعتراضي ببساطة على هذا الإجراء. فماسحات الأجساد هي الشكل النادر للتعقُّب غير المميِّز الذي لا يكون سرّياً، لذلك أغتنم الفرصة لضمّ صوتي إلى من يعارضونها. أنا أعتبرها مماثلة لإعادة تدوير النفايات في المنـزل؛ من غير المحتمَل أن تغيّر الصفائحُ والقناني التي أفصلها بامتثال مصيرَ الكوكب. والأميال التي أقطعها بسيارتي هي أكثر سوءاً، من الناحية البيئية، ولكن إعادة التدوير هي مدخل إلى المخدرات من نوع ما: تجعل تغيّراتٍ أكبر تبدو في متناول اليد.

كلّي أمل في أن تؤدي اعتراضاتي الصغيرة على الخصوصية إلى أن تكون تغيّرات أكبر في متناول اليد.

لا أستسلم للخوف . من المحتمَل أن تنتهي بـي خطوات أتخذها لحماية خصوصيتي إلى قائمة راية حمراء تحتوي على مشتبَه بهم محتمَلين.

لقد ناقش مدّعون عامون فيدراليون في قضية أريزونا مسألة عدم توقّع المتَّهَم حماية خصوصيته بشكل منطقي لأنه استخدم اسماً زائفاً بهدف الحصول على بطاقة لاسلكية مُسبَقة الدفع.

وتُظهر مستندات وكالة الأمن القومي التي كشف عنها إدوارد سنودن أن الوكالة تخزّن اتصالات مشفَّرة لمواطنين أميركيين، عِلماً أن توجيهاتها الخاصة تقول إن "الاتصالات المحلية تُتلَف بسرعة". ولكن يمكن الاحتفاظ بالرسائل التي تحتوي على "معانٍ سرّية"، مما يعني أن رسائل بريدي الإلكتروني المشفَّرة قد تضعني على قائمة راية حمراء من نوع ما لدى وكالة الأمن القومي.

ولكنني لا أريد الاستسلام للخوف من أن تضعني أعمالي لحماية الخصوصية على قائمة مراقبة. بدلاً من ذلك، أخطط لاعتبار تلك الرايات الحمراء جزءاً من اعتراضي السياسي على شبكات التعقُّب.

á á á

بطريقة ما، يكون هذا العالم الجديد الذي أَدخله مألوفاً للمخالفين في

أنظمة قمعية: عالَم حيث المحادثات الهادئة في مقهى تكون أكثر أماناً من الاتصالات الهاتفية، ورسائل البريد الإلكتروني، واتصالات إلكترونية أخرى.

لفهم الحياة التي أحياها، اتصلت برجل تفحَّص بعمق التحديات التي يواجهها المخالفون - مايك بيري، مطوِّر برامج كمبيوترية في توب برودجكت، يضع برامج مصمَّمة لمساعدة الناس على الإفلات من الرَّقابة. فبعد 11/9، صُدم بيري باجتياحات إدارة بوش للخصوصية، لذلك شرع بالتطوع كواضع برامج كمبيوترية لـتور. وبدأ بأخذ الخصوصية على مَحمل الجَدّ.

عندما كان ينظر إلى معلومات تقنية على أمازون مع رب عمله ومدير الهندسة، انـزعج لدى رؤية توصياتٍ بكتب تعالج مواضيع سياسية وشخصية، وقد أُضفي على التوصيات طابع شخصي. فاعتبر أن توصيات أمازون شخصية أيضاً بالنسبة إليه، لذلك شرع بمحو أثر بياناته.

التقيتُ وبيري في حديقة عامة في سان فرانسيسكو - (الأماكن العامة جيدة في الظاهر لإجراء أحاديث خاصة ما دمتم لا تستعملون كلمات مثيرة مثل متفجرة تدفع الناس على الإصغاء بحذر، وفقاً لجون شتروشز). كان بيري يبدو موضوع نقاشكم الأساسي عن المتسللين إلى الملفات الكمبيوترية - نحيل، شاحب قليلاً، ومرتدٍ ملابس سوداء. فأطلعني على بعض أسس أمنه العملانيّ (بالرغم من عدم إطلاعي عليها كلها، غير أنها تشمل أمنه الذاتي).

يصف بيري نفسه بـ"النباتي المتشدد حيال الرَّقابة" - ويعني بذلك أنه متشدد حيال تجنّب الرَّقابة بقدْر تشدّد النباتيين حيال تجنّب المنتجات الحيوانية. (لديه استثناءان: ما يزال يحجز تذاكر لرحلات جوّية وينـزل أحياناً في فنادق باسمه الحقيقي).

حتى إن أصدقاءه المقرَّبين لا يعرفون مكان إقامته، عِلماً أن بعضهم تبعه إلى مجمّع سكني في المدينة حيث يُقيم. (زارته عائلته ذات مرة ولكنهم لا يملكون العنوان الصحيح). لقد دسّ أحد أصدقائه في حقيبته هاتفاً محمولاً مُسبَق الدفع مزوَّد بنظام تحديد المواقع العالمي في مسعى عقيم لتحديد مكان إقامته.

هو يتلقى البريد في عدة أماكن، بما فيها مؤسسة لغسل الملابس، وصندوق بريد شركة يو بيي أس، وصندوق بريد تجاري يسمح له باستلام طرود بأسماء أخرى. ويستخدم أيضاً هواتف في المتناول. هو يدفع نَقداً لقاء هواتف مُسبَقة الدفع مخصَّصة لعلاقات مختلفة: واحد لعمله الرسمي، واحد لعمله الخاص، وآخر للاتصال بـتور. "أحاول تخصيص هواتف مختلفة لمواضيع مختلفة"، قال لي. هو يحاول إخراج البطاريات من الهواتف عندما

لا يستخدمها.

يؤمن بيري باستخدام عدة هويّات تخصَّص كل منها لعمل ما. يعني ذلك أنه يُعِدّ سلسلة بريد إلكتروني وعناوين للإرسال الفوري. بعد حديثنا، أعدّ عنواناً للإرسال الفوري مخصصاً لي كي أراسله. قال إنه سيلغيه بعد إنهاء أحاديثنا.

لقد بدت حياة بيري مليئة بالتحديات، فسألتُه عن أثرها عليه.

"صِدقاً"، قال، "لقد أثّرت في قدرتي على إقامة علاقات وثيقة". قال إن تقنياته لتجنّب الرَّقابة ساهمت في انفصاله عن حبيبتَين، وصعّبت عليه متابعة الاتصال بعدة أصدقاء لا يريدون إبقاء برنامجِ مسامَرة مشفَّر مفتوحاً كي يتحدثوا إليه.

وبدأ الأمر يبدو كما لو أنها مهنة شاب. بالرغم من كل شيء، بيري عازب يعمل من منـزله. أنا والدة مع طفلَين يتطلبان عناية خاصة كل يوم. سيكون من الصعب عليّ إدارة شؤون حياتي من مؤسسة لغسل الملابس مع هاتف لكل شخص أتواصل معه.

ولكن بطريقته اللطيفة، أكد لي بيري أنه يقوم بالمهمة بشكل خاطئ بأية حال، وأنه لا يتعيّن عليّ أن أكون نباتية متشددة حيال الرَّقابة. "بعض الأشخاص مرينين حيال الرَّقابة، وهو أمر جريء أيضاً"، قال.

بعد ذلك، استقل القطار المحلي معي إلى المكان الذي أقصد. وخرج برفقتي من المحطة إلى مرآبـي، ومن ثم عاد إلى داخل النَّفق، متوجّهاً إلى منـزله - أينما كان.

الفصل السادس

التدقيق

"يُفترض بك أن تعرفي بياناتك"، قال لي مايكل ساسمان أثناء فطور متأخر في مقهى قرب كابيتول هيل.

كان ساسمان، وهو مدّعٍ عام فيدرالي سابق في دائرة الجرائم الكمبيوترية والمِلكية الفكرية في وزارة العدل، قد بقي خارج منـزله في الليلة السابقة. قاد ساسمان، وهو أحد مُعجَبـي بروس سبرينغستين المخلصين، برفقة زوجته مدة ساعتَين ونصف لرؤية الرئيس يعزف في شارلوتسفيل، فرجينيا. كان ساسمان أعمش العينَين، ولكنه وافق بلطف على مساعدتي لرفع مستوى أمني الكمبيوتري إلى الدرجة الفُضلى.

"الأمر مُمِلّ"، أقرّ، ولكن التدقيق هو أول أمر يقوم به لزبائنه. ساسمان هو الآن شريك في مؤسسة المحاماة بركينـز كوي حيث يقدّم النُّصح للشركات، مثل غوغل، حول مسائل الخصوصية على الإنترنت. "نستهلّ بمخطط هيكلي، ومن ثم نبدأ باكتشاف كل جزء من البيانات التي تجمعها هذه الشركة من كل مصدر"، قال لي.

لقد تطرّق إلى نقطة هامة: إذا لم أكن أعرف مكان بياناتي، كيف يمكنني حمايتها؟ بالنسبة إليّ، لم يكن التحدي تحديد مكان بياناتي داخلياً، بل خارجياً. لذلك، قررت الشروع بالسعي إلى الخصوصية من خلال محاولة العثور على بياناتي.

á á á

لقد بدأتُ بمصادر البيانات الأكثر جلاء - غوغل، فيسبوك، تويتر، وهي الشركات التي دعوتها متبارون بأسلوب حر. ماذا تعرف عني؟

للعثور على بياناتي في غوغل، زرت موقع واجهة تحرير البيانات، وهو مشروع مراوِغ لغوغل يسمح للمستخدمين بالحصول على البيانات التي خزّنوها لدى غوغل. مستخدمةً قائمة إظهار في واجهة تحرير البيانات، حصلت على الاتصالات التي أجريتها مع 2,192 شخصاً عبر البريد الإلكتروني منذ بدئي باستخدام بريد غوغل عام 2006. وحصلتُ أيضاً على عدد قليل من الصور الفوتوغرافية التي خزّنتُها على بيكاسا (Picasa) (خدمة الصور الفوتوغرافية على غوغل، وكنت قد نسيت أنني استعملتها). وسحبتُ اثنَي عشر مستند تشاطرتها مع أشخاص يستخدمون غوغل درايف (Google

Drive) (ولكن ليس المستندات الـ204 كلها التي شاطرني إيّاها آخرون).

وعندما حاولت تحميل السجل التاريخي للمواقع التي زرتها، أعلنت واجهة تحرير البيانات: "لا سبيل حالياً لتجنّب السجل التاريخي لمواقع الويب على غوغل".

لقد عثرت على قليل من المعلومات على لوحة تحكّم غوغل - صفحة تحتوي على معلوماتٍ عن نشاطاتي، عبر مواقع خدمات متنوّعة توفّرها غوغل، مدفونةٍ في إعدادات حساب بريد غوغل الإلكتروني. وأشارت لوحة التحكم إلى أن الشخص الذي أجريتُ أكبر عدد من الاتصالات به عبر بريد غوغل من بين الأشخاص الـ2,192 هو زوجي - لم يفاجئني الأمر. وأشارت أيضاً إلى 23,397 رسالة بريد إلكتروني ومسامَرة أُجريت على بريد غوغل.

لم يكن السجل التاريخي لبحثي على الويب موجوداً على لوحة التحكم الخاصة بـي، وبدا الأمر غريباً. كان مخبَّأً في جزء من حسابـي يدعى أدوات أخرى. هناك، وجدت أن غوغل يسجّل أبحاثي على الويب منذ أن فتحتُ حسابـي عام 2006. من الواضح أنني أُجري نحو ستة وعشرين ألف بحث على غوغل في الشهر!

لقد ساعدني قيام غوغل بفرز أبحاثي وفقاً للتاريخ والفئة (خرائط، سفر، كتب، ألخ)، ولكنه نفاذٌ مُرعب إلى داخل ما يدعوه البوذيون "عقل القرد"، بسبب قفزي من مكان إلى آخر بدون راحة.

تأمّلوا بـ30 تشرين الثاني/نوفمبر 2010: استهلّيت اليوم بقراءة بعض أخبار التكنولوجيا. من ثم، وجدت نفسي فجأةً أبحث عن هرر صغيرة زهريّة اللون متلألئة لأجل ابنتي. انتقلت بعد ذلك إلى المعجَم للبحث عن كلمة لأجل المقالة التي أكتب، ومن ثم إلى أوبن تايبل OpenTable لتسجيل حجز في مطعم، وزرت أخيراً الكونغرس للحصول على نص التشريع المرتبط بالخصوصية. بِئس الأمر.

لم تُثِر أبحاثي أفكاري الباطنية فحسب، بل كشفت أيضاً عن أماكن وجودي. لقد أجريت مجموعة أبحاث عن خارطة مدينة برلين أثناء رحلتي إلى برلين؛ كان هيات ريجنسي بيون وسط رحلتي السنوية لرؤية حَمْوي وحماتي في الهند؛ بحثتُ عن مطار دي أف دبليو، إيرفينغ، جادّة تي أكس 3510 بينكلي، دالاس، تي أكس 75205 أثناء رحلة عمل إلى دالاس.

فهذا الأمر أكثر حميمية من دفتر يوميات؛ كان نافذةً داخل أفكاري كل يوم. وشعرت بالحنين أثناء اطّلاعي على أبحاثي التي أجريتها عن وسادات ر ضاعة بعد ولادة ابني، وعن مطاعم مكسيكية جيدة أثناء إجازة

عائلية في أريزونا.

أردت حقاً نقل البيانات، ولكنني لم أجد سبيلاً إلى ذلك بسهولة. قال لي ناطق بلسان غوغل، "هناك منتجات كثيرة ليست جزءاً من قائمة إظهار - بدأنا بخمسة منتجات عام 2011 وهي تزداد باطّراد". وأضاف أن باستطاعتي محو السجل التاريخي لموقعي على الويب. ولكنني عندما رأيته، لم أشأ محوه. أردت امتلاكه.

كانت فيسبوك خَدومة بنسبة أقل مع بياناتي. فنقرتُ على مهمة أَجرِ نسخة عن بياناتي، وأرسلَ لي فيسبوك أرشيفاً يمتاز بما لا يتضمّنه من معلومات. فهو لا يتضمن قائمة أصدقائي، منشوراتي، إعجاباتي، أو تعليقاتي على منشورات أشخاص آخرين، بل على صور فوتوغرافية قليلة ظننتُ أنها مُحيت، أشخاصٍ كنت قد محوتهم، وقائمة شاملة بتاريخ ومكان تسجيل دخولي إلى حسابي على فيسبوك (في الغالب، منزلي، مكتبي، وبضع رحلات عمل). وتبيّن أن منشوراتي وإعجاباتي موجودة في قسم آخر من فيسبوك يدعى سجلّ النشاطات. ولكنه ناقص أيضاً على نحو غريب. فسجلّ نشاطاتي يحتوي على بضعة منشورات، ولا وجود لأية إعجابات وتعليقات، ولا يمكن نقله.

كانت بياناتي على فيسبوك صورة باهتة لِما جرى مع ماكس شريمز عندما حصل على بياناته من فيسبوك عام 2011. لقد طلب شريمز، وهو طالب في فيينا، بياناته من فيسبوك وفقاً لقوانين الخصوصية الأوروبية وتلقّى 1,222 صفحة من البيانات الشخصية. لم تكن تتضمّن قائمة بكل أصدقائه فحسب، بل منشوراته أيضاً، وسواها، إضافةً إلى كثير من البيانات اعتقد شريمز أنه محاها - طلبات أصدقاء رفَضها، ووكزات كلامية ألغاها، وآراء محاها.

وفي آب/أغسطس 2011، تقدّم شريمز بشكوى مع لجنة حماية البيانات الإيرلندية (مكاتب فيسبوك الأوروبية موجودة في إيرلندا) زاعماً أن مقداراً كبيراً من البيانات التي تخزّنها فيسبوك تنتهك قوانين الاتحاد الأوروبـي لحماية البيانات. فالاتحاد الأوروبـي يطلب من مالكي البيانات الشخصية أن يكونوا شفّافين في ممارساتهم لجمع البيانات، والاحتفاظ بها ما دام ذلك ضرورياً لخدمة الغاية التي جُمعت لأجلها، وليس لغايات أخرى.

نتيجةً لذلك، راجعت اللجنة الإيرلندية ممارسات فيسبوك وأوصت ببعض أفضل الممارسات، بما في ذلك شروحات أفضل لسياساتها حول المحتوى المُلغى. بعد عام، غيّرت فيسبوك سياسة استخدام بياناتها وأعلنت بوضوح أن

"المعلومات المرتبطة بحسابكم سيتم الاحتفاظ بها ما دام حسابكم غير مُلغى". في العام 2012، راجعت اللجنة الإيرلندية إذعان فيسبوك ووجدت أن الشركة طبّقت معظم اقتراحاتها. ولكن الوكالة وجدت أن فيسبوك ما تزال ممتنعة عن القيام بإلغاء مُثبَت للحساب "دون ترك أي مجال للشك".

باختصار، بدا الأمر كما لو أن فيسبوك خططت للاحتفاظ ببياناتي - سواءً ألغيتها أم لا. ولكن، من غير المحتمل أن أحصل في وقت قريب على مجموعة شاملة من بياناتي على فيسبوك.

كان حصولي على معلوماتي من تويتر سهلاً. لقد ضغطت ببساطة على زر اطلُبوا أرشيفكم، وأرسلت لي تويتر على الفور بريداً إلكترونياً مع جدول بيانات إكسل يحتوي على 2,993 تغريدة منذ فتح حسابي عام 2008.

لم يكن الأمر بهذه السهولة. لم تكن تويتر تمنح المستخدمين أية فرصة للحصول على كامل أرشيفهم من التغريدات حتى العام 2012 - عِلماً أنها دأبت منذ العام 2010 على توفير بيانات مماثلة للشركات التي تدفع لقاءَ اشتراكها في مجموعة بيانات تويتر بأكملها بهدف مراقبة التطورات.

كانت تغريداتي أقل حميمية من أبحاثي على غوغل. فالعديد منها امتداد لعملي - مقالات يغرّدها زملاء أو أغرّدها بنفسي، وتغريدات مباشَرة في مناسبات. ولكن هناك بعض التغريدات التي نسيتُها كتلك التي أجريتها في 9 أذار/مارس 2009: "أول ليلة في عام كامل أنام فيها حقاً - نام طفلي أخيراً طوال الليل. يا للروعة".

بالإجمال، أعدّ المتبارون بأسلوب حر صورة جميلة مُلهِمة عن حياتي في السنوات القليلة الماضية. كانت أكثر شمولاً من أية ملفات راجعتُها في أرشيف الشتازي.

ومع ذلك، لقد جعلني قسم كبير منها أشعر بالحنين، بالرغم من القشعريرة التي اعترتني. إنه سجلّ رقمي عن حياتي.

لقد أعادتني إلى زمن لقائي مصادَفةً بصديقتي وزوجها في ملعب الأطفال في حيّنا في مانهاتن. فأثناء مشاهدة ابنتَينا - في السنّ نفسها - تلعبان على مجموعة القضبان الحديدية الأفقية والعمودية، سألني زوجها عن المقالات التي وضعتُها عن الخصوصية.

"اعتدت إيلاء اهتمام أكبر بالخصوصية"، قال. كنت واثقة من أنه سيُتبِع ذلك بعبارة "لا شيء لديّ أُخفيه"، ولكنه فاجأني بمقاربة مختلفة تماماً. قال إنه أدرك "إعجابه بفكرة ترك تُحف" عن حياته أكثر من قلقه في شأن الخصوصية. باختصار، قال، كل هذه البيانات تؤمّن "الخلود".

ناظرةً إلى تغريداتي القديمة وأبحاثي على غوغل، لم أتمالك نفسي عن التفكير في حديثي إلى زوج صديقتي. فمن بين كل مبرِّرات إقامة مجموعة بيانات كلّية الوجود، بدا الخلود مبرِّراً جيداً.

á á á

لقد ألقيت نظرة سريعة أخرى على الخلود عندما استرقت النظر إلى المعلومات التي يمتلكها وسطاء البيانات عني. حدث هذا الأمر أثناء جلوسي على منصة مايك غريفين المُشرِفة على خليج تشيزبيك في ضواحي بالتيمور.

يعمل مايك في ميدان وضع اليد على مشتريات لم يسدَّد ثمنها، ووجد نفسه عالقاً في فخ رَقابة السيارات. هو طويل القامة، نحيل، ومليء بطاقة عصبية المِزاج. يبدو أنه يعيش على القهوة والسجائر.

كنت أُجري بحثاً عن مقالة تتناول نشوء قارئات لوحات التسجيل المؤتمَتة، وقررتُ زيارة مايك. هو يدير إحدى أكبر العمليات الخاصة في الولايات المتحدة لالتقاط صور للوحات التسجيل. فأسطول سياراته المجهَّزة بكاميرات يقطع مسافة تتراوح ما بين ثلاثمئة وأربعمئة مِيل في اليوم، ماسحاً اللوحات في مناطق بالتيمور والعاصمة واشنطن. كل شهر، يجمع سائقوه الموزَّعون على فريقَي عمل بيانات عن مواقع مليون لوحة.

يستخدم مايك بشكل أساسي البيانات لمراقبة السيارات التي يُراد استعادتها بسبب عدم تسديد ثمنها. لقد عززت التكنولوجيا وضع يده على خمس عشرة سيارة في الليلة الواحدة، مقارَنةً مع نحو ست سيارات في الليل دون استخدام كاميرات. ولكن مايك يقول إن هدفه النهائي بيع حق ولوج بياناته للضامنين بكفالة، ولجامعي بيانات، ولمحقِّقين خاصين، ومؤمِّنين. "في السنوات الخمس التالية، آمل في أن تكون تجارتي الرئيسية جمع البيانات"، قال لي.

هو يفكّر في شارٍ محتمَل للبيانات: شركة تدعى تي أل أو. لقد سمعتُ عن الشركة طوال سنوات. فالمؤسس، هِنك آشر، أُسطوري. وقد تحوّل من مهرّب سابق للمخدرات إلى متحمّس لإنفاذ القانون، وأصبح الأكثر توهّجاً في تجارة البيانات.

جنى آشر ملايين الدولارات من خلال امتلاك مؤسسة تطلي ناطحات سحاب في فلوريدا، وتقاعد في الثلاثين من عمره. انتقل إلى غرايت هاربور كاي في الباهاماس، وقاد مركباً سريعاً، وطائرة أيروستار ذات محرّكَين، وطوّر عادة تعاطي الكوكايين. في النهاية، وبعد موافقته على نقل شِحنات قليلة من الكوكايين إلى فلوريدا جوّاً، أدرك أنه ذهب بعيداً. فأقلع فجأةً عن

تعاطي هذا العمل وقرر تنظيف الجزيرة من تهريب المخدرات.

شرع بالعمل في إدارة مكافحة المخدرات الأميركية، ولاحظ أن الوكالة بحاجة إلى قواعد بيانات أفضل. في العام 1992، أطلق منتَجاً يدعى أوتوتراك (AutoTrack) بدّل صناعة جمع البيانات.

كان أوتوتراك طريقة فُضلى للبحث في سجلات عامة: اشترى آشر بيانات من إدارة المركبات الآلية في ولاية فلوريدا وسهّل عملية البحث فيها. فجأةً، صار بإمكان الشرطة مراقبة قيادة السيارات وسجلاّت المركبات الآلية من خلال البحث فقط عن عنوان، أو رقم ضمان اجتماعي، أو جزء من اسم. في السابق، كان يتعيّن على الشرطة ولوج الاسم الكامل لشخص ما، وجنسه، وتاريخ ولادته، للحصول على لوحة. لقد بدّل أوتوتراك طريقة إجراء الشرطة تحقيقاتها، كما بدّل التحقيقات الصحافية. لقد استخدمتُ أوتوتراك عدة مرات للعثور على أسماء وعناوين أشخاص كنت أتحرّى عنهم.

ولكن توهّج آشر وسجلّه التاريخي في تهريب المخدرات لحقه وباع حصته في الشركة بقيمة 147 مليون دولار. محافظاً على عزيمته، سرعان ما اشترى آشر شركة أخرى مع منتَج مماثل جداً يدعى أكيورينت (Accurint). وبعد 11/9، وضع برنامجاً يدعى ماتريكس (MATRIX) ابتكر في ما بعد قائمة العامل الإرهابـي الخطير، ولكنه جنح بسبب الدفاع عن الخصوصية. مرة أخرى، استقال من شركته تحت الضغط.

في العام 2009، كان لآشر صَولة وجولة أخرى في هذا المجال، فأسس شركة قاعدة بيانات تدعى تي أل أو - الأخير (One Last TLO-The) لأنه المنتَج الأخير الذي خطط لإطلاقه. وتبيّن أنه كان مُحِقاً في ذلك؛ لقد توفّي عام 2013 عن واحد وستين عاماً.

قال مايك إن بيانات تي أل أو جيدة وأرخص من البيانات التي توفّرها لكسيس نكسيس، وكانت قد اشترت قبل سنوات شركتَي آشر السابقتَين. لقد حدّدت تي أل أو رسم 25 سِنتاً فقط لإجراء بحث بسيط، و5 دولارات لإجراء بحث متقدّم. بالمقارنة، حدّدت لكسيس نكسيس رسم 1,95 دولاراً لتقرير أساسي، و24,95 دولاراً لتقرير استثنائي.

سألتُ: "هل يمكنني رؤية تقريري؟".

أجابني: "بالتأكيد".

وفي أقل من دقيقة واحدة، كنت أحمل تقريراً من أربع صفحات يحتوي على كل عناويني السابقة - يعود تاريخها إلى رقم غرفة منامتي في الكلّية: #536بـي. لم تكن هناك أية معلومة خاطئة في التقرير.

لقد خطف ذلك نفَسي. كنت قد نسيتُ الرقم الموجود على باب غرفة منامتي، وعنوان المنـزل الجماعي في العاصمة واشنطن، كما نسيتُ مشاطرتي الغرفة مع خمس متخرجات حديثات العهد من الكلّية، ومدة إقامتي الوجيزة في شقة صغيرة في مدينة نيويورك قبل الانتقال إليها مع زوجي. لقد أعاد كلُّ عنوان موجة من الذكريات.

كان ذلك، بطريقة ما، أعمق من البيانات التي يملكها المتبارون بأسلوب حر عني. بالرغم من كل شيء، إنها حياتي الحقيقية التي تعود إلى عقود مضت؛ إنه حديث عن الخلود.

á á á

أثناء طلب معلوماتي من وسطاء بيانات آخرين، فقدتْ قصتي الغرامية مع الخلود زخمها. لقد أعددت قائمة بأكثر من مئتَي وسيط بيانات تجاري، وكنت على ثقة تامة بأنني لم أستعن بهم كلهم. لا يمكن اعتبار ذلك خلوداً، بل عُهراً.

كان بعضها ذائع الصيت، على غرار وكالة إكسبيريان التي توفر تقارير ائتمانية. ولكن معظمها مؤسسات صغيرة في تجارة البحث عن المعلومات البَصباصة - مواقع على الويب تسمح للناس بالبحث عن معلومات حول أشخاص آخرين لقاء رسم صغير، أو مجّاناً في بعض الأحيان لقاء إعلانات بيع.

هناك عقبات قليلة جداً لولوج تجارة البحث عن معلومات. تأمّلوا بقصة BeenVerified.com . ففي العام 2007، قرر جوش ليفي وروس كوهين عرض خدمة رخيصة لتفحّص الخلفيات على الإنترنت. وأنشأ الاثنان عملاً استثمرا فيه 200,000 دولار. وفي العام 2011، قالت الشركة إن مداخيلها بلغت 11 مليون دولار بستة عشر موظفاً ليس إلا. ليست نتيجة سيّئة إذا تمكنتم من تحقيق ذلك.

لا تخضع تجارة البيانات الأميركية لقوانين على نطاق واسع، والأمر معاكس في دول أوروبا الغربية. فهذه الدول تطلب من كل جامعي البيانات تمكين الأفراد من ولوج بياناتهم، والقدرة على تصحيح أخطاء في البيانات، وحق إلغاء البيانات في بعض الحالات.

بعد قراءة الأحرف الطباعية الصغيرة على 212 موقع ويب، أدركت أن 33 منها فقط تعرض عليّ فرصة رؤية البيانات التي تحتفظ بها عني. ولكن لدى إجراء تفحّص دقيق، لم تكن كل العروض حقيقية. فالبعض منها يطلب مني إنشاء حسابات بهدف رؤية بياناتي.

لقد اتصلتُ بثلاثة وعشرين وسيط بيانات وحصلتُ على بياناتي من ثلاثة عشر منهم. وطلب مني بعضهم إرسال طلباتي عبر البريد مُرفَقة بنسخة عن رخصة سَوقي، وسمح لي آخرون بإرسال طلبات عبر البريد الإلكتروني. تلقّيت معظم الإجابات من أكبر اللاعبين في هذه الصناعة.

أرسل لي إبسيلون، وهو أحد أكبر المسوِّقين المباشَرين الذي تبلغ مبيعاته السنوية 3 بليون دولار، تقريراً متفرّقاً من صفحتَين يحتوي على اسمي، عنواني، عمري، وانتسابي السياسي. لقد تضمّن قائمة فئات حديثة العهد لإجراء صفقات ضمن قوائم واسعة النطاق للغاية - ألبسة، وسائل إعلام، مؤسسات تجارية، صحة، وظائف منـزلية، ورياضات. والمعلومة الأكثر دقة هي وصف لاهتماماتي المنـزلية: ركوب الدراجة، ركض، ورياضات. بالنسبة إلى من لم تركب دراجة طوال خمس سنوات، بدا الأمر طموحاً أكثر منه واقعاً.

لقد صُدمت عندما طلب مني أكسيوم، عملاق جمع البيانات الذي تبلغ مبيعاته السنوية نحو 1,1 بليون دولار، إرسال شيك مصرفي بقيمة 5 دولارات كرسم للحصول على بياناتي. ولكنني أرسلته على مَضض. بعد شهر، أرسلت لي أكسيوم تقريراً من تسع صفحات يحتوي على رقم ضماني الاجتماعي، وتاريخ مولدي، ورقم بطاقة تسجيل الناخب، وعناوين يعود تاريخها إلى سنّ الطفولة. لم تزوّدني أكسيوم بأية معلومات تتناول اهتماماتي وتقوم ببيعها. إن تردّد أكسيوم في المشاطرة مغيظة بصفة خاصة لأنها تتفاخر في تقريرها السنوي بأنها تملك أكثر من "3,000 مَيل لكل مستهلك أميركي تقريباً". وأحد منتجاتها الرئيسية هو قاعدة بيانات برسونيك أكس (PersonicX) الذي يجمع الناس في سبعين مجموعة ضمن واحد وعشرين مرحلة من حياتهم.

بفضل الصحافي دان تينان الذي يقوم بعمل رائع في تغطية مسائل الخصوصية، عثرتُ على صفحة في موقع أكسيوم على الويب يسمح لكم بولوج عمركم، الوضع العائلي، الدخل، وعمر الأبناء، لتحديد المجموعة التي تنتمي إليها في برسونيك إكس. وعندما ولجت معلوماتي الحقيقية (مخيفة قليلاً)، أبلغني أكسيوم بأننا في مجموعة تدعى "ثروات وعائلات" - "إحدى المجموعات الأكثر ثقافة وثراء". فالأشخاص الموجودون في هذه المجموعة ارتادوا على الأرجح كلّية وتخرّجوا منها (أجل) وهم آسيويون (أجل، زوجي آسيوي). وهناك معلومة صحيحة أيضاً: "حياتهم الناشطة تجعل التسوّق عبر الإنترنت ضرورة وليس خياراً". ولكن صورة السلالة في مجموعة "ثروات

وعائلات" سخيفة قليلاً - صورة رجل وامرأة واقفَين أمام طائرة خاصة. لسنا أثرياء لدرجة امتلاك طائرة خاصة؛ حتى إننا لسنا أثرياء من درجة رجال الأعمال. نحن من طبقة الذين يحجزون مقاعد في أدنى سعر من الدرجة الأولى على متن الرحلات الجوية.

ولمجموعات أخرى في أكسيوم أسماء مثل "شحن وتصميم أزياء"، "رفيعو الثقافة متزوجون"، "متدافعون في المدن"، "طائفون في الريف"، و"أسلوب حياة مُسرِف". ولكن المجموعة التي نسبتني إليها أكسيوم مجهولة لأن موقعها الإيضاحي على الويب لا يطلب أسماء. لقد أدخلت أكسيوم في وقت لاحق خدمة عبر الإنترنت تسمح للناس برؤية بياناتهم إذا أدخلوا أسمهم، عنوانهم، تاريخ مولدهم، عنوان بريدهم الإلكتروني، وآخر أربعة أعداد من رقم ضمانهم الاجتماعي. لقد ترددتُ في الكشف عن هذا القدْر من المعلومات الحساسة، ولكنني وافقت على مضَض مرة أخرى وكشفت عن معلوماتي. نجم عن ذلك بيانات ديموغرافية ضئيلة بشكل ملحوظ: قالت أكسيوم إنني والدة آسيوية عزباء مع ابن في السابعة عشرة من العمر يقود سيارة تويوتا كورولا من طراز العام 2009 - كلها معلومات خاطئة. ولكن بيانات التسوّق مثيرة للإعجاب: تشير بشكل دقيق إلى أنني أفضّل التسوّق عبر الإنترنت على التسوّق دون الاستعانة بالإنترنت، وحدّدت فئات أنفقتُ فيها مالاً، مثل شراشف، سِلع منـزلية، و"ملابس نسائية - ملابس داخلية وجوارب".

لقد تطلّب الأمر ثلاثة أشهر كي تردّ داتالوجيكس على طلبـي، هي التي تدّعي تحقيق بيانات عن "كل أسرة أميركية تقريباً، وأكثر من تريليون دولار من العمليات التجارية التي يقوم بها المستهلكون". ولكن ذات يوم، وصل مغلف فيديكس من داتالوجيكس يتضمّن ورقتَين تحتويان على قائمة بـ"مجالات الاهتمام". كان خليطاً غير مرتَّب. أجل، أنا "والدة" و"ذَوّاقة طعام" و"متسوّقة عبر الإنترنت" لـ"أزياء وملابس النساء"، ولكن دعوتي "شديدة الاهتمام بالأزياء" و"شابّة وعلى الموضة" هو أمر بعيد عن الواقع.

بشكل مماثل، تشتري عائلتي مصابيح مقتصدة للطاقة وحليباً عُضوياً، ولكنني تفاجأت من وضعنا على قائمة "المستهلكين الخُضر" ومشترِي "الطعام الصحي". وبعض البيانات خاطئة تماماً: لا حيوانات أليفة لدينا ولا تلفاز، لذلك لم نشترِ أبداً أية "مستلزماتِ حيواناتٍ أليفة" ولم نشاهد "تلفزيون اللغة الإسبانية".

كانت فئات أخرى لداتالوجيكس غامضة بطريقة متعمَّدة. ووجدتُ أن

"وجهات النظر السياسية" و"الجغرافيا السياسية" هما من الفئات التي أُبدي اهتماماً بها، ولكن التقرير لم يكشف عن وجهات نظري باعتقادهم. بصورة مماثلة، أُدرج دخل أسرتي وقيمة منـزلي كفئتَين دون الكشف عنهما.

لقد أرسلت لي إينفوغروب بريداً إلكترونياً فقط يحتوي على اسمي وعنواني - المعلومات نفسها التي كنت قد وفّرتُها لولوج ملفّي. آه، شكراً.

وحصلت على نتائج أفضل من لكسيس نكسيس، وهو عملاق آخر في هذا الحقل. فبعد أربعة أيام من التقدّم بطلبـي، أرسلت لي لكسيس نكسيس عبر البريد الألكتروني عشر صفحات مجانية تتضمن "تقرير أكيورينت الشخصي" الذي يحتوي على كل عنوان أقمتُ فيه منذ العام 1989.

فعلى غرار تقرير تي أل أو، كان دقيقاً على نحو مشوِّش. لقد سجّل الشهر الواحد الذي قضيته في منـزل والدَيّ أثناء بحثي عن شقة في سان فرانسيسكو عام 1996. والتقط الشهرَين اللذَين قضيتهما في عُلّية رب عملي أثناء عملي كصحافية مُقيمة في واشنطن بوست عام 1992. وفي خانة "شركاء محتمَلون"، أُدرج زوجي ووالدته، وتواريخ زيارته له في شقته في نيويورك.

كان وستلوو التابع لتومسون رويترز الأكثر سخاء، وقد أرسل لي تقريرَين مجانيَّين: "موجَز" من أربع وثلاثين صفحة تحتوي على معلومات دقيقة في الغالب باستثناء ذِكر شقيقي بأنه رب أسرتي، وتقرير "شامل" من ثماني صفحات يُدرج لوحة تسجيلي، معلومات عن رَهن، ومستخدِم. فتقرير وستلوو الشامل هو التقرير الوحيد الذي ذكر المصادر التي حصلت منها على عناويني التاريخية - كلها من وكالات توفّر تقارير ائتمانية.

وبدت عروض بعض الشركات لولوج بياناتها أكثر من مجرد عرض بضائع في واجهة. لقد عرضت إنتليوس، أحد أكبر مواقع البحث عن أشخاص عبر الإنترنت والتي سجّلت في العام 2010 مبيعات بقيمة 150 مليون دولار (العام الأخير لتوافر هذه المعلومات علَناً)، موقعاً على الويب يدعى TrueRep.com يسمح للمستخدمين برؤية بياناتهم. ولكن الخدمة لم يُعلَن عنها في أيٍّ من مواقع إنتليوس التي عثرتُ عليها. وعندما زرت TrueRep.com للعثور على بياناتي، لم ينجح الأمر. بعد اتصالي بالشركة، أصلحتِ الخطأ وتمكنتُ من ولوج بياناتي - تعيّن عليّ أولاً الإجابة عن مجموعة من الأسئلة الشخصية، كتاريخ بناء منـزلي وموديل السيارة التي أقود. لكن التقرير لم يورِد أيّ تفصيل عن منـزلي وسيارتي، وهو أمر غريب. من الواضح أن إنتليوس تملك مزيداً من المعلومات التي لا تكشف

عنها، عِلماً أنها أوردت في تقريرها الأسماء الصحيحة لوالدَيّ، وزوجي، وشقيقي. ولكن كان هناك عنوانان خاطئان لي - أحدهما في البرونكس والآخر في الأمم المتحدة.

مع ذلك، كان وسطاء البيانات دقيقين في شأني إلى حد كبير. لقد حدّدوا معظم عناويني واتصالاتي بدقة، ونجحوا في تمييزي بأنني أمّ عاملة مستعجلة ميّالة لتفضيل الملاءمة على الادّخار.

á á á

أَمِلتُ في العثور على معلومات أكثر دقة في ميدان واحد من ميادين وساطة البيانات المنظَّم - صناعة تحديد مخاطر الائتمان انطلاقاً من تقرير ائتماني.

فقانون التقرير الائتماني العادل، الصادر عام 1970، يفرض على كل من يستخدم تقريراً ائتمانياً وأنواعاً أخرى من التقارير تزويدَ الناس بإشعار إذا كانوا يواجهون "إجراءً مؤذياً" كرفض طلب عمل تقدّموا به، أو رفض عقد تأمين، أو قرض، بسبب بيانات في التقرير. يجب على ذلك الإشعار توفير معلومات عن جامع البيانات الذي يوفّر المعلومات. ولكن الناس لم يتمكنوا، حتى الماضي القريب، من ولوج تقاريرهم بسهولة دون تعرّض طلبهم للرد.

في العام 2003، أقرّ الكونغرس قاوناً يفرض على أكبر ثلاث وكالات موفِّرة للتقارير - ترانسيونيون، إكسبيريان، وإكيفاس - تمكين الناس من ولوج تقارير ائتمانية على AnnualCreditReport.com سنويّاً وبشكل مجّانيّ. ولكن تلك التقارير المجانية لا تتضمن "التحديد الفعلي لمخاطر الائتمان" الذي يتم الاستناد إليه لتكوين فكرة عن المستهلكين.

وعندما طلبتُ نسخة مجّانية لتقريري الائتماني من ترانسيونيون، التقطتُ أول إلماعة بأن البيانات خاطئة عندما لم أتمكن من الإجابة بدقة عن السؤال الأمنيّ المخصَّص للتحقق من هويّتي: "أيّ مستخدِمَين من المستخدِمين الخمسة عملتِ لصالحهما؟" لقد عملتُ لصالح شركة واحدة فقط مُدرَجة على القائمة، ولكنني لم أتمكن من تخطّي ذلك السؤال حتى اخترتُ شركتَين. وهكذا، اخترت شركة بطريقة عشوائية ودخلت إلى تقريري. همممم، إجراءات أمنية كثيرة. (يتبيّن أنها لم تكن الحالة الوحيدة التي يلاحَظ فيها سهولة التحايل على الأسئلة الأمنية. ففي أذار/مارس 2013، تبيّن أن المتسلّلين إلى الملفات الكمبيوترية أجابوا عن أسئلة أمنية وحصلوا على تقارير ائتمانية خاصة بشخصيات عامة بدءاً بالسيدة الأولى ميشال أوباما

ومدير الأف بـي آي روبرت مويلر، وانتهاءً بالمشاهير بيونسيه وباريس هيلتون، وقد نُشرت عبر الإنترنت).

عندما دخلتُ تقريري الائتماني، وجدت أنه يُدرجني كعاملة لدى شركة تدعى بورجومي 1 إينك. منذ 1/30/2011. وأظهر بحث سريع على الويب أن بورجومي 1 إينك. موزّع مياه معدنية مقنَّنة من جمهورية جورجيا، مركزه بروكلين. وفي التقرير أيضاً عنوان سابق مموَّه لي: "30406920304 تي 75 مبنى 79".

لم تكن خبرتي غير عادية. لقد أظهرتْ آخر مراجعة لدقة التقارير الائتمانية قامت بها لجنة التجارة الفيدرالية أن 26 بالمئة من الناس عثروا على خطأ كبير واحد، على الأقل، في تقرير واحد على الأقل من تقاريرهم الثلاثة.

á á á

سرعان ما عثرت على بيانات أكثر سوءاً عني في زاوية غير منظَّمة من صناعة وساطة البيانات - تجارة تحديد مخاطر البيانات.

لقد عثرت بالصُّدفة على هذ الميدان عندما تلقّيت بياناتي من شركة تدعى إي بيرو. كان تقريراً من صفحة واحدة يشير إلى أن لا أبناء لي، ولم أُتِمّ الدراسة الثانوية، ويبلغ مدخولي 35,000 دولار - كلها بعيدة عن الواقع.

بقليل من البحث، اكتشفت أن إي بيرو حديثة العهد في حقل تحديد مخاطر الائتمان - حيث تستخدم الشركات بيانات شخصية متوافرة على نطاق واسع لوضع الناس في فئات جديدة. هناك شركات تُحلل شعبية تغريداتكم ومنشوراتكم على فيسبوك لتحدّد ما إذا كنتم "مؤثِّرين". وهناك مجموعة شركات تهدف إلى استخدام مصادر بيانات جديدة - كالشخصية أو السلوك عبر الهاتف المحمول - لتطوير تحديدات بديلة لمخاطر الائتمان.

تحاول إي بيرو، القائمة في شيكاغو والتي تأسست عام 2004، بناء تحديدٍ أفضل لمخاطر الائتمان، وقد جمعت 38 مليون دولار من رأسماليين لأجل نظام التحديد التنبُّؤي الخاص بها. تقول الشركة إنها تحلل معلومات عن أشخاص وتتنبّأ بـ"إمكانية الاتصال بهم" و"العلاقة المستقبلية الكاملة مع الزبون" كي يتمكن المسوّقون من اتخاذ قرار في شأن من يستهدفون. وتروّج إي بيرو لتحديداتها، قائلةً إنها تساعد الناس ذوي تواريخ مصرفية وائتمانية محدودة للحصول على خدمات مالية، وتسمح لجامعي الديون بالتنبُّؤ بإمكانية جمع ديون على حسابٍ عبر الإنترنت. تقول إي بيرو في نشرة

تسويقية تتناول "تخمين الدَّخل" إن بالإمكان استعمال تحديداتها لتقييم "المرضى الذين قُبِلوا في المستشفيات مؤخراً وأهليّتهم للانتساب إلى البرنامج الرعائي للجمعيات الخيرية".

وعندما اتصلتُ بـإي بيرو في شأن عدم دقة بياناتي، تلقّيتُ بريداً إلكترونياً من "استجابة إي بيرو" يشير إلى أن بعض بياناته يقع في خانة التقديرات. علاوةً على ذلك، أشارت الشركة إلى أنها "تحصل على معلوماتها من مصادر طرف ثالث، وأيٌّ من إي بيرو أو مزوّديها بالمعلومات، أو الباعة، أو مُعطي الرُّخَص، أو العملاء، أو المؤسسات الفرعية، لا يضمن دقة المعلومات أو خلوّها من الأخطاء". وقالت إن باستطاعتي عدم الاشتراك إذا كانت المعلومات غير دقيقة؛ لقد استفدتُ من العرض.

كانت شركة بايكو الأكثر بَعثاً على القشعريرة، مدّعيةً أن باستطاعتها تحديد نوعية شخصيتي بالاستناد إلى اسمي وعنواني فقط. في معلوماتها التسويقية، تقول بايكو إنها ابتكرت "خوارزمية تعتمد هندسةَ عكس البيانات المتوافرة عن سلوك الناس - علاقات، عمليات تجارية، نشاطات، اهتمامات، هوايات، السلوك لدى الشراء، وهكذا دواليك". تحصل بايكو على بيانات من وسطاء البيانات الكبار، وتحلل بعض قرارات الحياة وتترجم ما يمكن أن تعنيه لشخصيّتكم. على سبيل المثال، قد يعني الزواج استعداداً للالتزام، وتستخدم من ثم تلك البيانات لتحديد أمور مثل ما إذا كنتم اجتماعيّي الميول أو انطوائيين، أو إذا كنتم قادة لا أتباعاً.

تقول بايكو إنها وضعت نِبذات لبالغين بقيمة 181 مليون دولار. ولكنها قالت إنها لم تضع نِبذة عني.

á á á

أخيراً، حاولتُ استخراج بياناتي من الحكومة الأميركية. من الواضح أن وكالة الأمن القومي لم تكن لِتزوّدني بملفاتي (حاول آخرون وأخفقوا في الحصول على تلك الملفات)، ولكن يمكن لبعض الوكالات الأخرى تزويدي بها.

يمنح قانون الخصوصية، الذي أُقِرّ عام 1974، الأفراد حق رؤية ملفاتهم الحكومية وتصحيح المعلومات في تلك الملفات إذا لم تكن صحيحة. ولكن هناك ثغرة عملاقة في قانون الخصوصية: يمكن للوكالات إعفاء نفسها من بنود القانون.

نتيجةً لذلك، ليس من السهل على الأفراد أن يحصلوا على ملفاتهم. تأمّلوا بقصة إحدى قاطنات أوهايو، وتدعى جوليا شيرسون التي اعتُبرت "مسلّحة وخطرة" و"إرهابية مشتبَه بها" عندما وصلت بسيارتها إلى الجمارك

الأميركية ونقطة تفتيشٍ لحماية الحدود بعد قضاء نهاية الأسبوع في كندا عام 2006. لقد اعتقلها العملاء الفيدراليون مع ابنتها البالغة من العمر أربع سنوات طوال ساعات قبل إطلاقهما.

أرادت شيرسون التي اهتدت إلى الإسلام معرفة سبب وضعها على قائمة مراقَبة الإرهاب. لذلك، طلبت ملفاتها من الجمارك ومن وزارة الأمن الداخلي عملاً بقانون حرّية المعلومات وقانون الخصوصية. ولكن البيانات التي تلقّتها لم تتضمن سبب استهدافها. فقاضت الوكالات بسبب انتهاك قانون حرّية المعلومات وقانون الخصوصية. كان ردّهم بأنهم أُعفوا من توفير معلومات مرتبطة بقائمة المراقبة.

حصلت شيرسون على بعض المستندات عام 2008، ولكنها لم تتمكن أبداً من معرفة سبب نعتها بالخطرة والإرهابية. عام 2011، حكمت محكمة الاستئناف الأميركية للدائرة السادسة بأن الحكومة قد تُعتبر مسؤولة أمام القانون إذا احتفظت بشكل غير قانوني بسجلات النشاط الذي يحميه التعديل الأول. وأُحيلت القضية إلى محكمة أدنى. في العام 2013، توصّلت شيرسون إلى تسوية في شأن الأضرار التي لحقت بها، وذلك بعد أكثر من سبع سنوات من المعارك القانونية.

مع ذلك، تصوّرتُ أنني سأطّلع على ما يمكنني الحصول عليه عن نفسي. فطلبت ملفاتي من الأف بـي آي وأُبلغت بأنها لا تملك أية سجلات عني (بئس الأمر!) وبأن هذا الجواب "لا يؤكد أو ينفي وجود اسم الموضوع الخاص بك على أية قائمة مراقبة".

وثَبُت أن الطلب الذي تقدّمت به إلى الجمارك الأميركية ووكالة حماية الحدود كان مثمراً. فبعد نحو ثلاثة أشهر من التقدّم بطلبـي، تلقّيتُ مغلّفاً سميكاً مليئاً ببيانات - رد سريع نوعاً ما وفقاً للمعايير الحكومية.

وبهدف الحصول على مساعدة لتفسير الملفات، اتصلت بإدوارد هاسبروك، وهو كاتب سفريات مستقل مركزه سان فرانسيسكو، عمل في صناعة السفر طوال خمسة عشر عام. كان قد طلب سجلاته الخاصة بعد كشف وكالة الجمارك الأميركية في تشرين الثاني/نوفمبر 2006 عن شروعها باستخدام نظام سجلات يدعى نظام الاستهداف المؤتمَت يُعِدّ سجلات سفر للمواطنين الأميركيين بهدف "تخمين المخاطر". لقد تقدّم بطلب للحصول على سجلات نظام الاستهداف المؤتمَت عام 2007 وجدّد طلبه عام 2009. بعد عام، قاضى الوكالة، زاعماً أن رفضها تقديم ملفاته الكاملة انتهاك لقانون الخصوصية. لقد خسر الدعوى عندما قالت محكمة فيدرالية إن قيام

الجمارك باستثناء ملفاته من قانون الخصوصية هو إجراء شرعي حتى بعد طلب الحصول عليها. وافق هاسبروك على الاطّلاع على ملفاتي ومساعدتي على فك شيفرتها.

كانت الصفحات الثماني الأولى من قاعدة بيانات تي إي سي أس - نسخة مطوَّرة ومعدَّلة لـنظام اتصالات إنفاذ الخزينة السابق - وهو قاعدة بيانات خارقة من نوع ما تتضمن بيانات من أجزاء متنوّعة من وزارة الخزانة ووزارة الأمن الداخلي. كانت ملفاتي تحتوي على معلومات عن رحلاتي الدولية، وصولاً ومغادرةً، في تواريخ تعود للعام 1990. وفي كل عبور، تشير إلى المطار، والتاريخ والتوقيت، وفئة معتَّمة تدعى "نتيجة" قال هاسبروك إنها إشارة، على الأرجح، إلى ما إذا كنت قد خضعت لغربلة ثانوية.

إنها نظرة مختلسة محدودة إلى سجلّي التاريخي في السفر. وتتضمن رحلاتي الجوّية وقتَ وصولي إلى قاعة الجمارك، ولكن ليس المكان الذي أتوجّه إليه أو المكان الذي أصل منه. وهناك عبور واحد فقط بالسيارة - عندما عبرتُ إلى داخل كندا من نياغارا فولز عام 2003.

وفي مجموعة ثانية من المستندات معلومات أكثر تفصيلاً عن أسفاري - واحد وثلاثون صفحة من المعلومات عن حجوزاتي لأسفار دولية مأخوذة من قاعدة بيانات تدعى بيي أن أر، أي سجلات اسم المسافر.

لم تكن هذه السجلات في متناول الحكومة. إنها سجلات تجارية تحتفظ بها شركات النقل الجوّي. ولكن بعد الهجمات الإرهابية في 11/9، أقرّ الكونغرس على عَجَل قانون سلامة الملاحة الجوّية والنقل الذي يُلزم شركات النقل الجوّي بتزويد وكالات الجمارك ببيانات الحجوزات التجارية "عند الطلب". وبطريقة نموذجية، سرعان ما أصبح "عند الطلب" يعني وجوب توفير شركات النقل الجوّي للوكالة ولوجاً إلكترونياً لكل قواعد بيانات حجوزات السفر.

الآن، تتبرّع شركات النقل الجوّي بشكل روتيني بحجوزات سفر زبائنها الدولية لـجهاز استهداف المسافرين الأوتوماتيكي للجمارك وحماية الحدود - يخمّن "المخاطر" التي يشكّلها المسافرون الأفراد على الولايات المتحدة. تقول الوكالة إنها تستخدم بيانات الحجز لمدة خمس سنوات، ولكنها تخزّنها لمدة خمسة عشر عام لغايات مرتبطة بمكافحة الإرهاب.

بعد 11/9، اعترضت الحكومات الأوروبية على هذا التغيير، مجادِلةً أنه ينتهك قوانين الخصوصية الأوروبية. وبعد معركة قانونية ودبلوماسية مطوَّلة،

قامت خلالها محكمة العدل الأوروبية بإبطال الاتفاقية لمدة وجيزة، استسلم الأوروبيون في نهاية المطاف ووقّعوا الاتفاق. بالرغم من كل شيء، لم يرغبوا في أن يفقد مواطنوهم حق السفر إلى الولايات المتحدة بدون تأشيرة دخول. لكنهم فازوا ببعض الامتيازات - هناك حدود لمدة تخزين الولايات المتحدة بيانات بيي أن أر واستخدامها، ولا يمكن ولوج بيانات حساسة إلا على أساس "كل حالة على حِدة.

لقد فهمتُ تلك المعركة عندما نظرت إلى ملفاتي. فكل سجلّ من سجلات بيي أن أر مفصَّل على نحو لا يصدَّق، ويحتوي على كل تفاعل بدءاً من إجراء الحجز الأساسي وصولاً إلى الصعود إلى متن الطائرة.

لقد ظهر رقم بطاقة ائتماني الكامل عدة مرات، على غرار عنوان بريدي الإلكتروني، وتاريخ مَولدي، ورقم جواز سفري، وكل أرقامي الهاتفية - العمل، المنـزل، والهاتف المحمول. وظهرت أيضاً معلومات عن المسافرين برفقتي - عنوان البريد الإلكتروني لزوجي، تاريخا مَولد ابني وابنتي، وكل أرقام جوازات سفرنا. فاسما صغيرَيّ (اللذان استُبدلا بـالطفل الأول والطفل الثاني) وطلبات وجبتنا هي المعلومات الوحيدة التي نُقِّحت، كما يبدو.

لقد فك هاسبروغ شيفرة التوجيهات الغامضة التي تستخدمها شركات النقل الجوّي للتواصل عبرها من خلال الأجهزة الكبيرة المتعددة المستخدمين. فـ" TCP-4PAX-RECLOC5CLMWQ/5BUOEM YY OSI " هي الرسالة التي تُنذر موظفي شركة النقل الجوّي بأن عائلتي تريد الجلوس معاً لتشكل مجموعة (TCP) من أربعة ركّاب (4 PAX) بالرغم من حصولنا على حجزَين منفصلَين برقمَي حجز مختلفَين (RECLOC).

لقد بدا أن وكالة سفر شركتي كانت تزوّد الحكومة الفيدرالية أيضاً بمعلومات. ففي رحلةٍ إلى لندن، أرسلت الوكالة إلى الجمارك حجزي في الفندق (فندق بلومسبرغ، سرير ملكة)، رقم بطاقة ائتمان شركتي وتاريخ انتهاء صلاحيتها، رقم هوية مستخدِمي، وشيفرة موازنة دائرتي، وشيفرة داخلية تشير إلى أنني "لست شخصية بارزة".

والأكثر تسبباً بالقلق قيام الوكالة بإرسال حقل "هدف الزيارة" للحكومة، وهو حقل البيانات الذي يملأه الصحافيون عندما يحجزون رحلة. وتُرسَل تلك المعلومات إلى رب عمل المراسل للموافقة عليها.

لحسن الحظ أنني مصابَة بذُهان ارتيابيّ فائق، لذلك دوّنتُ "مؤتمر" فقط أو "رحلة لنقل تقرير إخباري" في تلك الحقول. ولكنني واثقة من إمكانية قيام زملائي بتدوين أوصاف أكثر توسّعاً عن خططهم. فتخيُّل قيام

بعض المراسلين بكتابة شيء من هذا القبيل: "رحلة لنقل خبرِ لقاءِ فاضحِ الأسرار جون سميث في ماريلاند" ليس أمراً بعيد الاحتمال.

فاتصلت بمحامِينا في وول ستريت جورنال ، وتفاجأوا بإرسال خطط سفر المراسلين للحكومة. بعد النظر في الأمر، قالت لي ناطقة بلسان شركة النقل الجوّي إن المسألة غير متعمَّدة ومحصورة بالسفر الدولي على متن طائرة محدَّدة. فعلّقت جورنال سفرها على تلك الطائرة حتى التمكن من إصلاح ذلك الخلل التقني. "نعمل بشكل وثيق مع وكالة سفرنا لحلّ هذه المسألة بأسرع وقت ممكن"، قالت لي.

في غضون ذلك، كانت معلومات مفصَّلة عن رحلاتي الإخبارية قابعة في ملفات حكومية وتحلَّل للتحقق من خطري الإرهابـي، دون أن يكون بإمكاني القيام بأي شيء لإزالتها.

á á á

كان تدقيقي مشوِّشاً بعمق. لم أحصل سوى على مقدار قليل من المعلومات المتوافرة عني؛ حتى إن هذا المقدار الصغير شامل على نحو مقلق. فهو يتضمن:

l كل عنوان أقمت فيه مذ كنت في الكلّية.

- كل رقم هاتف سُجِّل باسمي يوماً.
- أسماء كل أنسبائي تقريباً (إضافةً إلى حَمْوي وحماتي).
- قائمة بنحو ثلاثة آلاف شخص تبادلتُ معهم رسائل بريد إلكتروني في السنوات السبع الماضية.
- سجلات عن نحو ستة وعشرين ألف بحث أجريته على الويب شهرياً منذ سبع سنوات مفروزةٌ في فئات مثل خرائط وتسوّق.
- لمحة عن عاداتي التسوّقية.
- اتصالاتي الداخلية مع مستخدِمي، وول ستريت جورنال ، عن خطط لوضع تقارير إخبارية.

لقد جمع وسطاءُ بيانات تجارية معظمَ بياناتي. ولكن باستطاعة شبكات تعقُّب حكومية جرفها بسهولة.

لم أستطع تمالك نفسي عن مقارنة بياناتي بملفات الشتازي التي أعدّوها عن حياة الناس برَقابة غير متطوّرة ونوافذ محدودة. حتى في أحلامهم الأكثر جموحاً، لم يكن جهاز الشتازي يتخيّل الحصول على هذا المقدار من البيانات عن المواطنين بجهد صغير.

الفصل السابع
خط الدفاع الأول

قبل أن تتسنى لي فرصة إطلاق مشروع حماية خصوصيتي، تمّ التسلل إلى ملفاتي الكمبيوترية.

كانت نهاية أسبوع عيد العمال في العام 2012. لقد اصطحب شقيقي وخطيبته صغيرَيّ للتخييم، وكنت وزوجي متحمّسَين لحصولنا أخيراً على فرصة للتسكع بمفردنا.

لقد استيقظنا بكسل صباح يوم السبت. وبما أننا لم نكن على عَجَلة من أمرنا، كالعادة، لإطعام الصغيرَين وتمرينهما على السباحة، جلست إلى طاولة جهازي الكمبيوتري للتحقق من البريد الإلكتروني والتويتر. لقد رأيت على الفور عدة تعليقات من أشخاص قالوا إنهم تلقّوا عدة نسخات لرسائل موجَّهة من حسابي على التويتر. فتحققت من رسائلي الموجَّهة ووجدت أنني وجّهت عشرات الرسائل لأصدقائي، طالبةً منهم الضغط على أدوات ربط.

ما حدث واضح: تمّ التسلل إلى حسابي.

"اعتذاراتي لأولئك الذين تلقّوا نسخات رسائل مباشَرة مني. لقد تمّ التسلّل إلى ملفاتي. أقوم بتنظيف الفوضى الآن"، غرّدتُ عند التاسعة وسبع وعشرين دقيقة صباحاً. لقد تطلّبني الأمر ساعة لمحو أكثر من مئة رسالة وُجِّهت من حسابي. لحسن الحظ، كان المدى الأقصى للضرر.

كان بإمكان الأمر أن يكون أكثر سوءاً. فكلمة مروري مُعجمية ومكوَّنة من ستة أحرف، وقد استخدمتها لكل حساب من حساباتي تقريباً منذ بدء تسجيل دخولي إلى الإنترنت. ربما حاول متسلّل بارع اختراق عدة حسابات أخرى، وتمكّن على الأرجح من اختراق تلك الحسابات أيضاً.

كنت أُدرك وجوب اتخاذي تدابير أكثر أمناً. فكوني مراسلة تغطّي الشؤون التكنولوجية، عرفتُ أنه يُفترض بي استخدام كلمات مرور طويلة ومعقَّدة، ويجب عليّ اعتماد كلمة مرور مختلفة لكل حساب. لكن الحقيقة المُحرِجة هي أنني استمرّيت بمناقشة أفضل استراتيجية لكلمة المرور طوال عام تقريباً. لقد فكرت مليّاً باعتماد جملة مرور وإدخال تغييرات طفيفة عليها لكل موقع على الويب، ولكنني قلقت من قيام عملية تسلّل واحدة بإرغامي على تغيير كل كلمة مرور. وتفحّصتُ أنواعاً متنوّعة من البرامج

الكمبيوترية لإدارة كلمات المرور، ولكنني لم أتمكن من اتخاذ قرار في شأن ما إذا كنت أثق ببرامج مجّانية أو مدفوعةِ كاملِ التكاليف في هذا الوضع، وقلقت في شأن تشغيل البرنامج على مختلف أجهزة الكمبيوتر التي أستخدمها في المنـزل والعمل. وفكّرتُ مليّاً أيضاً في استراتيجية اقترحها صديقي المتسلّل مايكل جيه. جيه. تيفاني - "طريقة المواقع" [3] - التي يمكنكم بواسطتها تعليم أنفسكم استظهارَ كلمات مرور طويلة جداً من خلال استخدام تقنيات ذاكرية اعتمدها الإغريق القدماء لتذكّر قصائد طويلة. ولكن كلما كلّمني عن مدى سهولة الأمر، بدا الأمر صعباً.

باختصار، لقد أصابتني مسألة كلمة المرور بالشلل لمدة عام تقريباً، مُبقيةً كل كلمات مروري في هذه الفترة عُرضة للتسلّل، مفكّرةً في عدم تغييرها حتى أضع استراتيجيتي المُثلى.

á á á

كان التسلل دعوة للاستيقاظ: قبل تمكني من معالجة مسألة الخصوصية، كنت بحاجة إلى تنقية مقاربتي للأمن.

فالخصوصية والأمن يُعتبران أحياناً على خلاف مع أحدهما الآخر. بالرغم من كل شيء، يُطلب منا باستمرار التخلي عن الخصوصية باسم الأمن. تأمّلوا فقط بأمثلة قليلة: ماسحات الأجساد في المطارات، برامج مسح الإنترنت بحثاً عن كلمات مفتاح إرهابية، كاميرات في كل زاوية من الشارع.

"لدينا قول مأثور في هذا المجال: الخصوصية والأمن لعبة محصّلتها صفر، قال إد جورجيو، وهو مستشار في شؤون الأمن عَمِل في وكالة الأمن القومي، لنيويركر ذات مرة.

لكن الخصوصية ليست شيئاً بدون الأمن، في الواقع.

"علينا أن نضع جانباً مفهوم أن حرّيتنا وأمننا قيمتان متعارضتان قائمتان على طرفَي متأرجحة متقابلَين، وأنه عندما تكون إحداهما في الأعلى لا بد من أن تكون الثانية في الأسفل"، قالت وزيرة الأمن الداخلي، جانيت نابوليتانو، في خُطبة لها عام 2012. "والواقع المؤلم للمسألة هو أنكم لا تستطيعون العيش بحرّية إذا عشتم بخوف. فالأمن شرط أساسي إذا رغبنا في ممارسة الحقوق التي نتعلّق بها".

كانت مُحِقة. فقبل أن أتمكن من حماية حرّياتي، كنت بحاجة إلى ضمان أمن نطاقي الرقمي. بالرغم من كل شيء، ما فائدة الدفاع عن نفسي من تعقُّب مميِّز إذا تركت نفسي مكشوفة للمتسللين ولتدخلات أخرى؟

لم أكن مستعدة لمدى ما بلغه هذا المشروع من صعوبة.

á á á

تتمثل المشكلة مع الأمن الكمبيوتري بأن معظم النُّصح الذي نُسديه منافٍ للعقل.

تأمّلوا بمسألة مصطادي الأطفال. عندما كنت أضع كتابي عن ماي سبيس (MySpace) عام 2008، كان مصطادو الأطفال على الإنترنت بُعبُع الساعة. وتمثّل النُّصح الموجَّه من كل الخبراء بالاحتفاظ بجهاز كمبيوتر العائلة في غرفة الجلوس، ومراقبة أطفالكم عندما يستخدمونه. إنه نُصح منافٍ للعقل يستحيل العمل به. فمعظم الأهل يعملون - سواءً يديرون شؤون مكتب أو يديرون شؤون أسرة. ومعظم الصغار يقومون بعدة أعمال متزامنة أثناء عملهم على جهاز كمبيوتر - يُنجزون فرضهم المنـزلي، ويوجّهون رسائل فورية لأصدقائهم، ويتصفّحون الإنترنت. ففكرة قدرة الأهل على الإشراف على كل تلك النشاطات أثناء تقاضي راتب يكفي لكَسْب رزقهم، ووضع العشاء على المائدة، هو أمر مثير للسخرية.

لقد بلغتُ حد اعتبار تحذيراتٍ كهذا التحذير مماثلةً للُصاقات التعريف على الفرشات التي تقول إنه من غير القانوني نـزع اللُّصاقة المخربَشة، أو اللُّصاقات على سِروالٍ مخمليّ مضلَّع تقول: **لا تُزيلوا هذه الرُّقعة!** فهذه اللُّصاقات مصمَّمة لفئة واحدة من الجماهير: المحامون. أما بقيّتنا فيتجاهلون اللُّصاقات بابتهاج أو يشعرون بالذَّنْب بسبب تجاهلها.

بصورة مماثلة، يستحيل العمل بالنُّصح الذي نتلقاه عن الأمن الكمبيوتري. تأمّلوا بالنُّصح الذي عثرتُ عليه أثناء بحث بسيط على الويب في شأن الأمن الكمبيوتري: سيِّروا برامج مضادة للفيروسات؛ أَعِدّوا جدار نار؛ انسخوا ملفاتكم؛ أَطفئوا شبكة الواي - فاي عندما لا تستخدمونها؛ لا تتصلوا بمواقع واي - فاي عامة إلا إذا كنتم تستخدمون التشفير؛ أَقفلوا جهازكم الحضني بسلك أمنيّ عندما تكونون في فندق (!)؛ تجنّبوا مواقع الويب التي تحتوي على جافا سكريبت (JavaScript)؛ أَزيلوا برامج كمبيوترية قديمة؛ لا تستخدموا مايكروسوفت آوتلوك (Outlook Microsoft) أو أدوبـي ريدر (Reader Adobe)؛ سجّلوا رقم تحديد هوية هاتفكم تحسّباً لفقدان هاتفكم أو سرقته. بعض هذه النصائح جيدة - نسخ الملفات والاحتراس من شبكات واي - فاي العامة، بصفة خاصة - ولكن بعض الأشخاص الذين ليسوا محترفين في شؤون الكمبيوتر يواجهون وقتاً صعباً أثناء فرز الضروري وغير الضروري.

هناك سبب واحد لكل هذا الإرباك: على صناعة الأمن الكمبيوتري أن تُخيفنا حقاً بهدف إقناعنا لشراء منتجاتها. من مصلحتهم المبالغةُ بوصف التهديدات. هل تذكرون الانصهار الكمبيوتري على مستوى العالم ككل في العام 2000 الذي لم يحدث؟

فكرة بيانية مثيرة للاهتمام: لا يتكل معظم المحترفين في الأمن الكمبيوتري على البرامج المضادة للفيروسات، بل يحدّثون برامجهم الكمبيوترية باستمرار ويدقّقون في اختيار تلك التي يريدون استخدامها. والأهم من ذلك أنهم لا يضغطون على أدوات ربط أو يفتحون مستندات إذا لم يكونوا واثقين تماماً من مصدرها. ويملك بعض المحترفين في الأمن الكمبيوتري الأكثر إصابةً بالذُّهان الارتيابـي معلوماتٍ قليلة جداً عن أنفسهم متوافرةً على شبكات التواصل الاجتماعي.

وكلمات المرور هي أفضل مثال على سُخف الأمن الكمبيوتري. فالحكمة التقليدية تقتضي قيامكم بتغيير كلمة مروركم كل ثلاثة أشهر؛ يُفترض تعزيزها بعدة رموز وأحرف؛ ولا يجب تدوينها في أي مكان.

يتم التعاطي مع هذه القواعد في مكتبـي كما لو أنها تعاليم إلهية. فكل ثلاثة أشهر، أتلقى بريداً إلكترونياً يذكّرني بإعادة تنضيد كلمة مروري. قبل الشروع بهذا النظام، كان لديّ كلمة مرور طويلة بشكل معقول - نحو أحد عشر حرف، إذا لم تخنّني الذاكرة. ولكن الضغط المتواصل لوضع كلمة مرور جديدة حطّ من براعتي. في العام 2012، استسلمتُ ووضعتُ كلمة مرور جديدة تحتوي على الشهر الذي أتلقى فيه رسالة البريد الإلكتروني التذكيرية. وهكذا، عندما وصلتني الرسالة التذكيرية لشهر أذار/مارس، بدّلتُ كلمة مروري إلى أذار 2012! (مع علامة التعجب الضرورية للإيفاء بعملية تنظيم الرمز). وفي حزيران/يونيو، بدّلتها إلى 2012حزيران؟، وهكذا دواليك. لقد خفّضتُ عدد المكوِّنات إلى تسعة يمكن معرفتها بسهولة.

هناك دليل كافٍ على أنني لست الوحيدة في تدوير زوايا كلمة المرور. ففي العام 2010، حلّل باحثون في الأمن الكمبيوتري قاعدة بيانات من اثنتَين وثلاثين مليون كلمة مرور (تمّ التسلل إليها ونُشرت على شبكة الإنترنت لمدة وجيزة) ووجدوا أن كلمات المرور الأكثر تمتعاً بالشعبية هي "123456" مُتبَعة بـ"12345"، "123456789"، و" password ". ووجد الباحثون في مؤسسة الأمن الكمبيوتري، إيمبرفا، أن نحو 30 بالمئة من كلمات المرور تحتوي على أقل من ثمانية حروف، وأن نحو 50 بالمئة تستخدم أسماء أو

كلمات معجمية. والنتيجة: "بعد 119 محاولة فقط، يلج المتسلل إلى حساب جديد في كل ثانية، أو يتطلبه الأمر 17 دقيقة لاختراق 100 حساب".

وتقترح دراسة أحدث عهداً تعود للعام 2013 أن تغييرات كبيرة لم تحدث. لقد وجد منظّم الاتصالات البريطاني، أوفكوم، أن نصف مستخدمي الإنترنت البالغين في المملكة المتحدة يستخدمون كلمة المرور نفسها في معظم مواقع الويب التي يزورون، إذا لم يكن في كلها. علاوةً على ذلك، قال 26 بالمئة إنهم استخدموا كلمات مرور يسهل اكتشافها مثل تاريخ مَولدهم أو اسمهم.

لقد استنتج علماء الكومبيوتر أيضاً، والحمد لله، أن كلمات مرورنا المريعة ليست خطأً يُحسَب علينا. ففي كتابه الدراسي المحترَم جداً هندسة الأمن ، يكتب روس أندرسون من مختبر الكمبيوتر في جامعة كامبريدج، "لقد اختُصرت مشكلة كلمة المرور بالتالي: اختاروا كلمة مرور لا يمكنكم تذكّرها، ولا تدوّنوها".

عام 2004، نشرت جمعية مهندسي الكهرباء والإلكترونيات دراسة عن "سهولة تذكّر كلمة المرور والأمن" - أندرسون أحد من ساعد على وضعها - تستنتج أن عيوب كلمات المرور ناجمة جزئياً عن التوجيهات التي يتلقاها الناس، إذا تلقوا أية توجيهات، لدى ابتكار كلمات مرور.

وأجرى واضعو الدراسة اختباراً على ابتكار كلمات مرور شمل ثلاثمئة طالب تقريباً. لقد طُلب من إحدى المجموعات ابتكار كلمات مرورها الخاصة بها على أن تكون مؤلَّفة من سبعة مكوِّنات على الأقل وتحتوي على مكوِّن واحد على الأقل لا يكون حرفاً. وسُلّم أفراد مجموعة ثانية ورقة تتضمّن أعداداً وأحرفاً، وطُلب منهم اختيار ثمانية أعداد وحروف بشكل عشوائي وبعيون مُغمَضة. وطُلب من مجموعة ثالثة ابتكار كلمة مرور بالاستناد إلى جملة يمكن تذكّرها، مثل " Its 12 noon I am hungry " (إنها الثانية عشرة ظهراً وأنا جائع) لوضع كلمة المرور " Is12Iah ". بعد ذلك، حاول الباحثون حلّ شيفرة كلمات المرور باستخدام تقنيات تسلّل متنوّعة. لقد كشفوا النقاب عن ثلث كلمات المرور في المجموعة الأولى (حيث ابتكر المستخدمون كلمات مرور دون تلقّي كثير من النُّصح)، وأقل من 10 بالمئة من كلمات المرور في المجموعتَين الأخريَين. "نقترح تغيير النُّصح المقدَّم للمستخدمين في شأن اختيار كلمات المرور"، استنتج الباحثون. في بعض الحالات، يُفترض إعطاء المستخدمين توجيهات عن كيفية وضع كلمات مرور يمكن تذكّرها، ومن الأفضل للمؤسسات، في حالات

أخرى، تحديد كلمات مرور ببساطة للمستخدمين. وقالوا، "نادراً ما يختار المستخدمون كلمات مرور يصعب معرفتها ويسهل تذكّرها".

عام 2010، حمّل علماء في كلّية لندن الجامعية السياساتِ المؤسساتية المتعلقة بكلمات المرور مسؤوليةَ وضع كلمات مرور سيّئة. ودرس واضعو الدراسة "استخدام كلمة المرور بشكل متهوّر" في موسستَين كبيرتَين ووجدوا أن قواعد كلمات المرور الصارمة بشكل مُفرط - إرغام المستخدمين على ابتكار كلمات مرور منيعة وتغييرها بشكل متكرر - تسببت بإجهاد المستخدمين وحملتهم على تدوين كلمات مرورهم، محبِطين بهذه الطريقة المساعي الأمنية. "عندما تفوق متطلبات السياسة المتبَعة قدرات المستخدمين، يُرغَمون على تطوير تقنيات أكثر تعقيداً - أو أقل أمناً - للتعاطي مع الوضع"، كتب واضعو الدراسة.

وبالمناسبة، يقول العديد من خبراء أمن الكمبيوتر إنه من الجيد تماماً تدوين كلمات مروركم ما دمتم تحتفظون بها في مكان آمن.

في العام 2005، تكلّم جيسبر جوهانسون، الذي كان مدير برامج أعلى آنذاك لسياسة الأمن في مايكروسوفت، في مؤتمر للأمن، ووبّخ الصناعة بسبب إسدائها نُصحاً سيئاً في شأن كلمات المرور. "كم عدد الذين يملكون سياسة كلمات مرور تقول إنه لا يجب عليكم تدوين كلمات مروركم وإلا تعرّضتم لعقوبة الموت؟" سأل جوهانسون. فرفع أغلب الحاضرين أصابعهم. "أُعلن أنه أمر خاطئ تماماً. أُعلنُ أنه يُفترض بسياسة كلمات المرور فرض تدوين كلمات المرور. لديّ 68 كلمة مرور مختلفة. إذا لم يكن يُسمح لي بتدوين أيٍّ منها، احزروا ماذا سأفعل؟ سأستخدم كلمة المرور نفسها. بما أن ليس كل الأنظمة تسمح بكلمات مرور جيدة، سأختار كلمة مرور رديئة حقاً، وأستخدمها في كل مكان ولا أغيّرها أبداً. إذا دوّنتُها ومن ثم حميتُ الورقة - أو أي شيء دوّنتها عليه - لا ضَير في ذلك. يسمح لنا ذلك بتذكّر مزيد من كلمات المرور وأفضلها".

لقد جعلني البحث أشعر بحال أفضل لجهة كلمات مروري الضعيفة. ولكنها لم تحلّ بعد مشكلتي المتمثلة بكيفية ابتكار عشرات كلمات المرور المنيعة.

بالرغم من كل شيء، هناك العديد من الجُمل التي يمكنني تذكّرها. والعديد من مواقع الويب ليست جديرة بجهدٍ عقليّ.

á á á

صباح اليوم الذي تمّ فيه التسلل إلى ملفاتي، غيّرت كلمات المرور إلى

حساباتي الرئيسية - البريد الإلكتروني، العمل المصرفي، شبكات التواصل الاجتماعي. وبدلاً من وضع كلمات مختلفة بواسطة أحرف كلمة مُعجمية واحدة مكوَّنة من ستة أحرف، أعددتُ مجموعات أطول مكوَّنة من أحرف، وأعداد، ورموز، ودوّنتها على الورق.

كان إجراء بديلاً مؤقتاً ليس إلا، وأعرف أن كلمات مروري ما تزال غير جيدة بما يكفي. إنها في الغالب كلمات مختلفة موضوعة بواسطة أحرف كلمة عامة واحدة. ولكن كلما حاولتُ التفكير في كلمات جديدة، يعجز عقلي عن ذلك. لقد ذُكِّرتُ بدراسة تدّعي أن 38 بالمئة من البالغين يفضّلون القيام بمهام منـزلية روتينية، كتنظيف مِرحاض أو غسل الأطباق، على ابتكار اسم مستخدم وكلمة مرور جديدَين.

وبعد أسابيع من عدم القدرة على ابتكار أي شيء، استسلمتُ، وقررت الاستعانة ببرنامج لإدارة كلمات مرور. معتمدةً على فلسفتي المتمثلة بـ"الدفع لقاء الأداء"، اخترت 1باسوورد (Password1) لأنه خدمة مدفوعة ومنقَّحة جيداً. وأمِلتُ في أن يعني ذلك أنها صفقة حقيقية توفّر خدمة جيدة للزبائن.

يدير 1باسوورد في الأساس كل كلمات مروركم؛ تخزّنون كل كلمات مروركم في برنامجه. يمكن ولوجه بكلمة مرور رئيسية واحدة. لا تخزَّن كلمات المرور في مكاتب 1باسوورد في كندا بل في ملف مشفَّر على جهازكم كي تكون كلمات المرور آمنة تماماً. وإذا نسيتم كلمة مروركم الرئيسية، تفقدون القدرة على ولوج كل كلمات مروركم. بمعنى آخر، يخضع 1باسوورد لاختبار بِركة الوحل.

إن وضع كل كلمات مروري على جهاز الكمبيوتر أمر مخيف، ولكنني اتخذت خطوة جريئة بسبب عدم قدرتي على ابتكار كلمات مرور. فأنـزلتُ البرنامج على جهازي وشرعت بعملية إدخال كلمات المرور التي أصادفها على الإنترنت.

إنها عملية بطيئة حقاً. كنت قد نسيتُ عدد مواقع شركات النقل الجوّي، والفنادق، والمواقع التجارية العشوائية التي لديّ حسابات فيها. في بعض المواقع، استخدمت منتِج كلمات المرور في باسوورد1 لابتكار كلمات بالطول المطلوب ومزج الأحرف، والأعداد، والرموز. وفي مواقع أقل أهمية، أدخلت ببساطة كلمة مروري الضعيفة ووعدت نفسي بتحسينها في وقت لاحق.

في غضون ثلاثة أشهر، حمّلتُ باسوورد1 واحداً وخمسين كلمة مرور.

ولكنني واصلت الاحتراس من وضع كلمات مرور حساسة، كتلك المرتبطة مثلاً بالعمل المصرفي والبريد الإلكتروني وملفات عمل هامة، في باسوورد1. لقد احتفظتُ بها على الورق. وواجهتُ مشكلة على الفور: لم أكن أملك أية فكرة عن ماهيّة كلمات مروري. فتلك التي ابتكرتها من خلال باسوورد1 هي مجرد سلسلة أحرف، وأعداد، ورموز غير مفهومة، مثل qwER43@! . وتلك التي وضعتها بنفسي كلماتٌ مكوَّنة من رموز وأعداد متداخلة، مثل Tr0ub4dour&3 . لم يكن من السهل تذكّر أيٍّ منها.

تفاجأتُ بمدى حاجتي المتكررة إلى كلمات مروري عندما أكون بعيدة عن جهازي الكمبيوتري. لقد اتصل زوجي ليسألني عن كلمة المرور لحسابـي على أمازون كي يتمكن من استخدام خدمة الشحن المجانية - وتعيّن عليّ أن أقول له إنني أتناول الغداء ولا أملكها. فوجّه لي رسالة عبر البريد الإلكتروني ليسألني عن كلمة المرور إلى أحد حساباتي التي أَلِجها تكراراً لأجل رحلاتي الجوية؛ لم أكن أملك كلمة المرور هذه أيضاً. عندما حصلت على هاتف محمول جديد، واصلت محاولة إعداد حساب لي على تويتر بعيداً عن طاولتي - ومن ثم أدركت أنني لا أعرف كلمة مروري إلى تويتر. (في باسوورد1 نسخة للهواتف، ولكنني شعرت بأن تخزين كل كلمات مروري على هاتفي محفوفة بالمخاطر).

لقد شعرتُ بالانـزعاج في بادئ الأمر، ولكنني أدركت أخيراً حقيقة الحاجات المُلِحّة لكلمات المرور هذه: حاجات غير مُلحّة. وثَبُت أن باستطاعة التغريدة الانتظار، وباستطاعة طلب بضائع عبر أمازون الانتظار أيضاً.

á á á

في غضون ذلك، شرعت بمحاولة ضمان أمن بياناتي بطرق أخرى.

لمحاربة انتحال الشخصية (المعروف أيضاً بسرقة الهويّة)، اشتريت آلة تقطيع أوراق وبدأت بتقطيع مستندات تحتوي على معلومات شخصية. واشتريت محفظة جَيب تصدّ إشارات تحديد الترددات الراديوية على بطاقاتي الائتمانية وجواز سفري التي يمكن للمتسللين تصفّحها.

ولضمان سلامة بياناتي من عملية تسلّل أكثر جدّية، اشتريت قرصاً صلباً خارجياً وشرعت بإجراء نسخات عن ملفاتي بانتظام. (أجل، لم يسبق لي أن أجريت نسخات؛ أمر رهيب، أعرف). ولإفشال المتسللين الذين قد ينجحون في اختراق جهازي، قمت بتشفير قرصي الصلب (على جهاز ماك، تُنجَز المهمة بكبسة واحدة).

لقد وضعت لُصاقة فوق كاميرا الويب كي لا يتمكن المتسللون من

استخدامها للتجسس عليّ عن بُعد. واشتريت مِرشَحاً لصيانة الخصوصية يحمي شاشة جهازي الحضني من الناس الذين يحاولون القراءة من فوق كتفي أو من المقعد بجانبـي على متن الطائرة.

ولمحاربة المتسللين الذين يحاولون سرقة كلمات مروري من خلال عمليات وصل واي - فاي في المقاهي، استعنتُ ببرنامج يدعى إيتش تي تي بيي أس إفريوير (HTTPS Everywhere) يضمن تشفير عمليات وصلي بالإنترنت كلما كان ذلك ممكناً.

وعملتُ أيضاً على أن أكون أكثر احتراساً لدى استخدامي الواي - فاي بصورة عامة. فبدلاً من الاتكال على جهاز واي - فاي لنقل رِزم بيانات بين شبكات الكمبيوتر (Router)، أضفتُ إلى جهازي الكمبيوتري وصلة إثرنت ذات برامج ثابتة. وأثناء السفر، بدأت باستخدام جهاز محمول يؤمّن ولوج الإنترنت من خلال واي - فاي (Hot spot). كان الاتصال متقطعاً أحياناً، ولكنه جعلني أشعر بأنني أفضل حالاً بكثير من الاتصال بكل أنظمة واي - فاي المتطفّلة تلك المعتمَدة في الفنادق التي تُرغم حركة اتصالاتكم عبر الإنترنت على المرور عبر أجهزتها.

لقد اعتمدت أيضاً أنظمة كلمات مرور مزدوجة - تُثبت صحة المعلومة من خلال عاملَين - متى توافرتْ. على بريد غوغل الإلكتروني، يعني ذلك استخدام تطبيق يزوّدني بشيفرة أُدخلها بالإضافة إلى كلمة مروري. في مصرفي، يعني ذلك البحث في إعدادات الإنترنت حتى أجد طريقة للحصول على رقم "سرّي" قبل السماح بأية دَفعات مالية.

ولكنني اعتمدت تلك الأنظمة في أماكن حيث لا أكون مضطرة للكشف عن رقم هاتفي. فتويتر توفّر خدمة التثبّت من صحة المعلومة من خلال عاملَين، ولكن للأشخاص المستعدّين فقط لتلقّي رسائل نصّية من تويتر - لذلك رفضت الأمر.

وحاولت أيضاً استخدام نظام يدعى ليتل سنيتش (Little Snitch) لمراقبة كل عمليات الوصل التي يحاول جهازي الكمبيوتري إجراءها، ولكنني تخلّيت عنه بسرعة. لقد ثَبُت في النهاية أنني لم أشأ في الواقع معرفة عدد عمليات الوصل التي يُجريها جهازي في أي وقت محدَّد. ووجدت أنه يتعيّن عليّ الموافقة على ست وسبعين عملية وصل كي أفتح متصفّحي على الويب، وأَلِج بريد غوغل الإلكتروني، وأبدأ بنقل دفق من الموسيقى عبر سبوتفاي (Spotfy). لقد بدا كل طلب على هذا النحو: "إسمح بعمليات وصل خارجة إلى المنفذ 80 (http) لـ d1hza3lyffsoht.cloudfront.net حتى

يتوقف سبوتفاي". وتمثّل خياراي بعبارتَي "إلى الأبد" أو "حتى يتوقف" فحسب. بعد ساعة اتخذتُ فيها سبعة وتسعين خياراً سيّئاً، أدركت أن لا فكرة لديّ عما يجري، وألغيت البرنامج.

أثناء تفحّصي الخيارات الأمنية، اعتبرت أن المشكلة الأكبر تتمثل بأنني لا أعرف بمن أثق. كنت أعرف ما يكفي لأحترس من المحاولات التهكمية للاستحواذ على خوفي. ولكنني لم أكن أعرف ما يكفي لاختبار المنتجات، في الواقع، والتحقق من أدائها.

حتى ذلك الحين، كنت أستخدم في الغالب أدوات أشخاص أعرفهم أو أدواتٍ أُثبتت كفاءتها. كنت أعرف وأثق بالتقنيين في مؤسسة الحدود الإلكترونية التي تُنتج برنامج إيتش تي تي بيي أس إفريوير. وليتل سنيتش برنامج ذائع الصيت. وبصورة مماثلة، أُثبتت كفاءة 1باسوورد. ولكنني لم أعرف كيف أكوّن رأياً عن مورد مشفَّر متوافر عبر الإنترنت يدعى سبايدرأوك (SpiderOak) وكنت أفكر فيه مليّاً. أردت تخزين بياناتي في الخدمة تحسّباً لحدوث خَطْب ما لنُسخاتي الاحتياطية، ولأتمكن من ولوج ملفاتي من أي مكان. ولكن سبايدرأوك لم يكن معروفاً بشكل جيد.

لم أتمكن من فهم الشركة جيداً من خلال موقعها على الويب. لقد وددتُ لو أنها لا تبدو كمعظم مواقع الأمن الكمبيوتري - تميل إلى إظهار خلفية سوداء والكثير من المراجع لـ"تشفير الرُّتَب العسكرية". يطغى على سبايدرأوك لون برتقاليّ مُشرِق ويروّج لـ"إمكانية ولوج المرء بياناته دون سواها"، وهو أمر مماثل لاختبار بِركة الوحل. لقد أوصى كريستوفر سوغويان، وهو تقنيّ في الاتحاد الأميركي للحريات المدنية، بسبايدرأوك أيضاً. ولكن موقعاً على الويب وتوصيةً هما بمثابة عَصيدة خفيفة بالنسبة إلى شخص يسعى للحصول على وجبة كاملة. لذلك، أرسلت بريداً إلكترونياً للمدير التنفيذي الأعلى، إيثان أوبرمان، واتفقنا على الالتقاء عندما أقوم بزيارتي التالية إلى سان فرانسيسكو.

لقد التقينا في مقهى على الموضة. بدا إيثان بشعره الأشقر وذراعَيه القويّتَي العضلات أشبه برياضيّ أكثر منه بمهووس بالكمبيوتر. لقد انتابتني الشكوك على الفور.

أثناء ارتشاف القهوة، روى لي قصته - بالفعل، لم يكن سردَ مهووس نموذجي بالكمبيوتر. لقد نشأ في ضاحيةٍ أرستوقراطية من ضواحي شيكاغو، وارتاد مدرسة داخلية إعدادية تدعى هوتشكيس، ومن ثم هارفارد. كان، كما بدا لي، لاعب هوكي وقائد فريق لاكروس في هارفارد. بعد تخرّجه عام

2000، عمل لصالح مؤسسة والده - تساعد ناشري المجلات على إدارة قوائم انتشارها ومبيعاتها. أرادت الشركة استراتيجية رقمية، لذلك وضع إيثان عملية تسويقية عبر البريد الإلكتروني ضمن شركة والده. ولكنه تعب من العمل لصالح مؤسسة العائلة بعد سنوات قليلة، فأخذ نفَساً وسافر، واشترى أيضاً أول جهاز كمبيوتر له من طراز ماكنتوش. وعندما تعيّن عليه الاتصال بوالدته ليطلب منها إرسال ملف له، عبر البريد الإلكتروني، من الجهاز الشخصي البُرجي الذي يضعه في خزانة والدَيه، أدرك أن هناك فرصة تسويقية.

كان هناك الكثير من "خدمات إجراء نُسخات" مثل إكس درايف (Xdrive) وموزي (Mozy)، ولكنها تعرض إجراء نُسخات لجهاز واحد فقط. لقد أراد أيضاً لبياناته أن تعمل بشكل متزامن على كل الأجهزة. "إجراء نُسخات ليس أمراً جذّاباً"، قال لي. "الأمر أشبه بفرك أسنانك. إن ولوج بياناتك في كل مكان هو الأمر الجذّاب حقاً".

لم تكن الجاذبية ما أبحث عنه تماماً؛ أردت مزيداً من التفاصيل عن إمكانية ولوج المرء بياناته دون سواها. لأجل ذلك، حوّلني إيثان ببهجة إلى شريكه في المؤسسة، آلن فيرِلس. (لإنصاف إيثان، لم يكن ربما معتاداً على الصحافيين الذين لا يريدون أكثر من مجرّد اقتباس جذّاب لمقالاتهم). مع ذلك، بدا إيثان كما لو أن الموارد المالية بين يدَيه. فقال لي إن الشركة تحقق أرباحاً وتجني مالاً من بيع اشتراكات بدلاً من بيع إعلانات. يلائم هذا الأمر مبدأي التوجيهي المتمثل بالدفع لقاء الأداء.

بعد أسبوعَين، تحدّثت عبر الهاتف إلى آلن فيرِلس، شريك إيثان والرئيس التنفيذي لشؤون التكنولوجيا في سبايدرأوك. شرح آلن أنه أحد الذين حثّوا على تشفير البيانات. "كان من المهم بالنسبة إليّ أن تكون مشفَّرة قبل أن تغادر جهازي". وشرح كيف تأخذ سبايدرأوك كلمات مرور المستخدمين وتحوّلها إلى طرق تشفير فريدة. فالتشفير هام بأهمية كلمة المرور التي يبتكرها المستخدم. "لا شيء مُلزِم لجهة طول كلمة المرور"، قال. "قررنا أنه من غير الجيد حمل المستخدمين على تغيير طرق اختيار كلمات المرور إلى أجهزتهم بينما نُعلمهم بأن بياناتهم تضيع إذا نسيوا كلمات مرورهم".

نظراً لما عرفته عن كلمات المرور، قدّرت عالياً عدم قيام سبيادرأوك بإقحام المستخدمين في وضع حيث لا يمكن تحقيق أي مكسب. واستمالني آلن عندما قال لي إن "رفع مستوى الأمن الكمبيوتري إلى الدرجة الفُضلى

يتطلب منا حماية المستخدمين من أنفسهم، وثَبُت أنها طريقة جيدة لحماية المستخدم من بقيّة العالم". وقال إنه سبق للشركة أن تلقّت طلبات من أجهزة إنفاذ القانون لأجل الحصول على بيانات، ولكن عندما عرف الموظفون أن لا سبيل لسبايدرأوك كي يفك شيفرة البيانات، تراجعوا عن الطلبات.

وأطلقتُ تنهيدة ارتياح. لقد جعله الحديث المباشَر عن رفع مستوى الأمن الكمبيوتري إلى الدرجة الفُضلى وكلمات المرور مُقنِعاً بالنسبة إليّ. ونجحت سبايدرأوك في اختبار بِركة الوحل، وتسجّلتُ كي أشترك في برنامجها. ولكن الاختبار برمّته بدا طريقة حمقاء لتفحّص أداء الأمن الكمبيوتري. هل كنت سأقوم حقاً بزيارة كل مزوِّديَّ بالتكنولوجيا كي أحدد أمانتهم؟

وبعد كل ذلك، ما يزال أمني على سبايدرأوك يعتمد على طول كلمة مروري.

á á á

كان الأمر يتطلب بعض المهارة لتفكيك كلمة مرور. الآن، يمكن للجميع القيام بذلك.

لقد ساعدتِ القدرات الكمبيوترية المتزايدة مفكّكي كلمات المرور على العمل بسرعة أكبر. وسمح التوافر المتزايد لقوائم ضخمة تحتوي على كلماتِ مرورٍ مسرَّبة بقيام المبرمجين بوضع برامج تجعل عملية تفكيك كلمات المرور أكثر دقة. ولإظهار مدى سهولة الأمر، فكك الصحافي نيت أندرسون ثمانية آلاف كلمة مرور في يوم واحد، مستخدماً برنامجاً مجّانياً على الإنترنت يدعى هاشكات. "بالرغم من عِلمي بسهولة تفكيك كلمات المرور، لم أعرف أنه سهل على نحو مثير للسخرية - حسناً، يكون سهلاً على نحو مثير للسخرية عندما أتخطى رغبتي الشديدة في ضرب جهازي الحضني بمطرقة كبيرة، وأكتشف أخيراً ما أفعل"، كتب.

تتمثل طريقة تفكيك كلمات المرور بالتالي (نقاط مبسَّطة جداً):

1 يحصل المتسلل على قائمة كلمات مرور لتفكيكها.

- هذه القوائم مشفَّرة عادةً - أو "مخلوطة".
- بعد ذلك، يحاول المتسلل فك شيفرة الخليط.
- في العادة، يحاول المتسلل أولاً تسيير برنامج مُعجميّ لمقارنة نماذج الخليط بكلمات تقليدية مُعجمية.
- عندئذٍ، يقارن المتسلل نماذج الخليط مع قواعد بيانات ذائعة الصيت تحتوي على كلمات مرور مسرَّبة.
- يحاول المتسلل القيام بهجومٍ "قوة غاشمة" - تختبر خيارات في

جُمل بسيطة مثل " aaaaa "، ومن ثم " aaaab "، ومن ثم " aaaac "، إلخ.

إن هجمات القوة الغاشمة هي ما يدعوه الباحث في الأمن الكمبيوتري، روبرت غراهام، "مشكلة أُسّيّة. فمقدار الوقت المطلوب يزداد بسرعة بعيدة عن كل معقولية". لذلك السبب، يشنّ أندرسون هجماتِ قوةٍ غاشمة على كلمات مرور يبلغ طولها ستة أعداد فقط. ولو حاول تفكيك كلمات مرور مكوَّنة من تسعة أو عشرة أحرف لَتطلّبه تفكيكها أسابيع أو أشهراً. لقد تمكن من تفكيك ثمانية آلاف كلمة مرور فقط من مجموع سبعة عشر ألف كلمة مرور حاول تفكيكها. "العبرة واضحة: باستطاعتي تفكيك كل آخر خليط في الملف - ولكنني سأكون بحاجة ربما إلى جزء كبير من العام للقيام بذلك، مفترِضاً أن جهازي لم ينهار تحت الضغط"، كتب.

تتمثل إحدى العِبر في عالم تفكيك كلمات المرور بأنه يُستحسَن بالناس الذين يخزّنون كلمات مرور الاستعجال. إن أفضل ممارسة لهذه الصناعة هي بـ"إضافة بيانات عشوائية بهدف تعديل كلمات المرور" (Salt) - أي أنه إذا ابتكر المستخدم كلمة مرور من ستة أحرف، يتعيّن على الخالط إضافة عدة أحرف فريدة إليها، جاعلاً إيّاها أكثر طولاً، قبل أن يخلطها. من شأن ذلك أن يجعل عملية حلّ شيفرتها أكثر صعوبة.

للأسف، إن إضافة بيانات عشوائية بهدف تعديل كلمات المرور ليس أمراً مألوفاً بما يكفي: كشفت تسللات حديثة العهد على LinkedIn ، ياهو!، وإي هارموني (EHarmony) عن مجموعات نفيسة من كلمات المرور التي لم يُضَف إليها بيانات عشوائية بهدف تعديلها وتمّ حلّ شيفرتها بسرعة.

لأولئك الذين يتعيّن عليهم ابتكار كلمات مرور، إن العِبرة من عالم مفككي كلمات المرور بسيطة: أَعِدّوا كلمات مرور أكثر طولاً، وتجنّبوا كلمات معجميّة بسيطة أو كلمات مرور ذائعة الصيت (مثل 1باسوورد).

á á á

يدعو علماء الكمبيوتر قياسَ طولِ كلمة المرور "قياساً للقصور". فكلما كان قياس القصور عالياً ازدادت صعوبة الاختراق. قال لي جيفري غولدبرغ، وهو خبير كلمات مرور في أجيل بيتس، صانعي 1باسوورد، إن قياس القصور هو "قياس لعدد الطرق التي يمكنك من خلالها الحصول على نتيجة مختلفة باستخدام النظام نفسه". فلكلمات المرور القصيرة والبسيطة،

كالكلمات المُعجمية، قياسُ قصور منخفض جداً لأن اكتشافها أمر سهل. ولكلمات المرور الأكثر طولاً التي تحتوي على أنواع عديدة من الرموز، والأحرف، والأعداد، قياسُ قصور أعلى لأن اكتشافها يتطلب مزيداً من التخمينات.

كان جوليان أسانج يعرف هذا الأمر عندما ابتكر كلمة المرور التالية لقاعدة بيانات الرسائل البرقية ويكيليكس: #AcollectionOfDiplomaticHistory-Since-1996-ToThe-PresentDay هي بطول ثمان وخمسين مكوِّن، مع عدد قليل جداً من الرموز، ويسهل تذكّرها. بالطبع، إن سبب معرفتنا لكلمة مروره يعود لقيام صحيفة غارديان بنشرها في كتاب عن ويكيليكس. إذاً، من الواضح أنها لم تكن كلمة مرور آمنة من جوانب أخرى.

يصعب على نحو مُحبِط تقدير صعوبة قياس القصور. قد يكون لكلمة مرور طويلة قياس قصور منخفض إذا احتوت على كلمات بسيطة وقواعد لغة سهلة. وبدأ قياس القصور في كلمات المرور التي ابتكرتُها يستحوذ على عقلي. ذات يوم، كنت جالسة خارج حفلة رقص لابنتي عندما صادفتُ برنامجاً على الإنترنت لقياس القصور، وضعه دان ويلر، مهندس في دروفوكس. فبرنامجه يقيس قصور كل كلمة مرور، إضافةً إلى "المدة المطلوبة لتفكيكها"، فشعرتُ على الفور بإثارة اختبار كلمات مروري التي يمكن تذكّرها والتي وضعتها حديثاً. وشرعت بإدخال كل كلمات مروري بتهوُّر.

استهلّيت العملية بكلمة المرور إلى مصرفي (ابتكرتها من خلال استخدام اثنَي عشر حرفاً يمكن تذكّرها). أوه، الأمر مثير جداً. كان لديّ ست وخمسون بِتّاً يتعيّن قياس قصورها ويتطلب تفكيكها "قروناً"!

بعد ذلك، اختبرت كلمة مروري إلى بريد غوغل الإلكتروني التي ابتكرها 1باسوورد (ثمانية عشر مكوِّن). هي تحتوي على ثمانين بِتّاً يتعيّن قياس قصورها ويتطلّب تفكيكها "قروناً". ولكنني كنت أكره كلمة المرور هذه: لا يمكنني تذكّرها أبداً.

ولكن كلمة المرور إلى بريدي الإلكتروني الخاص بوول ستريت جورنال (تسعة مكوِّنات) كان مخيّباً للآمال. لقد ابتكرتها باستخدام طريقة تسهّل عملية تذكّرها، ولكنها تحتوي على ثمانية وعشرين بِتّاً فقط يتعيّن قياس قصورها. لقد تطلّب تفكيكها سبع ساعات ليس إلا!

أوه، يا إلهي. كيف يحدث هذا الأمر؟ فكلمة المرور التي أستخدم لحماية حسابـي على 1باسوورد (ناتج محلّي آخر يمكن تذكّره ويبلغ طوله

سبعة عشر مكوِّن!) تحتوي على سبعة وثلاثين بِتّاً يتعيّن قياس قصورها، ويمكن تفكيكها في مدة خمسة أشهر.

إنها رياضة إدمانية ولكن مسبِّبة للغمّ. كان هناك نموذج يتشكل - كلمات مروري التي يضعها باسوورد1 منيعة جداً؛ تَراوح ناتجي المحلّي من كلمات المرور بين المنيع والضعيف جداً.

وأسوأ ما في ناتجي المحلّي من كلمات مرور: يمكن تفكيك كلمة المرور التي تسمح لي بولوج جهاز الكمبيوتر في مدة أربع دقائق. و"بلحظة واحدة" يمكن تفكيك كلمة مروري التي تسمح لي بولوج مدوَّنتي.

ومع اضمحلال الإثارة المرافِقة لتفكيكها، أدركتُ أنه من الغباء التام إدخال كلمات مروري إلى نظام تفكيك غير معروف أثناء استخدام واي - فاي. فبالرغم من استخدامي جهازاً محمولاً يؤمّن ولوج الإنترنت من خلال واي - فاي، وعملية وصل مشفَّرة بالويب، وموقعاً يَعِد بعدم تخزين كلمات مرور، كان ما يزال بالإمكان أن ينتهي الأمر بكلمات مروري في قاعدة بيانات تستخدمها فِرَق تفكيك كلمات مرور.

لقد بات لديّ سببان لوضع كلمات مرور جديدة: (1) واقع أن كلمات مروري لا تتمتع بقياس قصور كافٍ و(2) غبائي.

á á á

في خضمّ بحثي عن كلمات مرور تتمتع بقياس قصور عالٍ، فكرت مليّاً في مجموعة واسعة من الخيارات، بما فيها كلمات مرور تُبتَكر باستخدام لغات مبهَمة وجُمل مرور كتلك المستخدَمة من قِبَل جوليان أسانج.

ولكنني صادفتُ ثانيةً مشكلة قدرتي الابتكارية. كان باستطاعتي وضع كلمة واحدة أو كلمتَين بلغة مبهَمة، أو جملة واحدة أو جملتَين، ولكنني علمت في النهاية بأن الأفكار ستفرغ مني وأبدأ باستخدام كلمات مرور ضعيفة.

تُظهر الدراسات أن الناس يميلون إلى اعتماد طرق مختصَرة حتى عندما يضعون كلمات مرور أطول. ففي العام 2012، درس الباحثون في جامعة كامبريدج استخدام جُمل مرور على Amazon.com ووجدوا أن العديد منها قائم على أفلام سينمائية أو موسيقى أو جُمل ذائعة الصيت، مثل "مجتمع الشعراء الخَدِرين"، "ليلة الكلاب الثلاثة"، و"معك أو بدونك". بالنتيجة، إن العديد من جمل المرور ضعيفة على غرار كلمات مرور عادية. "توحي نتائجنا أن المستخدمين غير قادرين على اختيار جُمل مكوَّنة من

كلمات عشوائية تماماً، ولكنها تتأثر باحتمال وضع جملة بلغة طبيعية"، كتب المؤلفان جوزف بونو وإيكاترينا شوتوفا.

أكدت الدراسة ارتيابـي: أنا بحاجة إلى نظام لا أكون مضطرة فيه للتفكير.

وعثرتُ على ما أحتاج إليه في نظام كلمات مرور يدعى دايسوير (Diceware). إنه بسيط على نحو مضلِّل: ترمي نَرداً سداسيّ الجوانب خمس مرات، وتستخدم النتائج لاختيار أعداد من قائمة كلمات دايسوير التي تحتوي على 7,776 كلمة إنكليزية قصيرة، كل منها مرقَّم. هي تبدو على الشكل التالي:

16655 clause (بند)

16656 claw (مِخلب)

16661 clay (صَلصال)

16662 clean (نظيف)

16663 clear (واضح)

16664 cleat (مَربَط حِبال)

16665 cleft (شِقّ)

16666 clerk (موظف كتابـي)

يوصي مبتكر دايسوير، أرنولد رينهولد، باستخدام سلسلة من خمس كلمات على الأقل. لذلك، تبدو كلمات المرور الناتجة على هذا النحو: alger puck blond curry klm . ويمكنكم جعل كلمة المرور أكثر مناعة بإضافة مزيد من الكلمات، أو بإضافة قليل من الأحرف أو الرموز أو الأحرف الكبيرة. ولكن أبسط سلسلة من دايسوير مكوَّنة من خمس كلمات يتألف كل منها من خمسة مكوِّنات تتطلب أكثر من ألف وثمانمئة يوم لتفكيكها، وفقاً لبروس مارشال، مؤسس PasswordResearch.com

فاستخدام دايسوير يضمن اختياركم الأعداد عشوائياً. وهناك أيضاً، بالطبع، برامج كمبيوترية ومواقع على الويب تولّد لكم أعداداً عشوائية. ولكن رينهولد وخبراء أمن آخرين يحترسون من استخدام برامج توليد أعداد عشوائية غير معروفة خشية أن تكون موضوعة من قِبَل أخصام يسعون إلى تفكيك نظام كلمات مروركم. في الواقع، تُظهر المستندات التي أطلقها إدوارد سنودن أن وكالة الأمن القومي وضعت أحد المقاييس العِلمية لمولِّد أعداد عشوائية يمكن اختراقها.

شاعرة بالحماسة جرّاء توقُّع عدم اضطراري للتفكير في كلمات المرور

مجدداً، طبعتُ قائمة كلمات دايسوير على سبع وثلاثين صفحة، وأحدثت ثقوباً في الأوراق، ووضعتها في غلاف. ولكنني خشيت من اضطراري لرمي النَّرد مئات المرات للحصول على كل كلمات المرور التي أحتاج لابتكارها. بقي الغلاف على طاولتي حتى راودتني فكرة بارعة: إشراك ابنتي البالغة من العمر ثماني سنوات، والمتنقلة في أرجاء المنـزل شاعرةً بالملل، في التقليد العريق للصغار أثناء الصيف بعد انتهاء العام الدراسي. فقلت لها إنني سأدفع لها لقاء إعداد كلمات مرور لي.

في غضون ساعة، سلّمتني ورقة تحتوي على خمس كلمات مرور من صنع يدويّ - وطلبت أَجرها نَقداً. فدفعت لها 3,50 دولاراً.

متحمّسة بالكسب السهل، وجّهتْ رسائل بريد إلكتروني لجدّها وجدّتها، وخالها، وقليل من أصدقاء العائلة لتُعلِمهم بأنها شرعت بمهنة صناعة كلمات مرور. وهذا ما كتبَته:

الموضوع: مهنتي [حرفياً]

أشرع بمهنة كلمات المرور الخاصة بـي حيث أُعِدّ كلمات مرور. تبلغ كلفة خمس كلمات مرور ثلاثة دولارات وخمسين سنتاً. خمس كلمات مرور في الصفحة الواحدة. آمل في أن تختبروها.

كتبت لي والدتي على الفور لتسألني عما إذا كان بريد ابنتي الإلكتروني قد تعرّض للتسلّل. فأكدتُ لها أنه عمل حقيقي، وتسجّلتْ للحصول على بعض كلمات المرور. في آخر الصيف، تبيّن أن ابنتي أعدّت نحو خمسين كلمة مرور للعائلة والأصدقاء، ورفعتْ أسعارها إلى دولار واحد لكلمة المرور الواحدة.

لقد شعرتُ بالإثارة. لديّ الآن مجموعة من كلمات مرور لا أعرفها مخزَّنة في 1باسوورد، ونحو عشر كلمات مرور منيعة يمكن تذكّرها لأجل حساباتي الأساسية. وكعلاوة غير متوقَّعة، تمكنتُ أخيراً من إقناع ابنتي بإيلاء الخصوصية عنايتها - أو على الأقل، إيلاء الاستفادة من الخصوصية عنايتها.

الفصل الثامن
التخلّي عن غوغل

في 8 حزيران/يونيو 2004، حضر عميل أف بـي آي إلى مكتبة عامة في دِمينغ، واشنطن، وطلب معرفة أسماء الأشخاص الذين ولجوا كتاب بن لادن: الرجل الذي أعلن الحرب على أميركا بقلم يوسف بودانسكي.

لم يسبق لأمر مماثل أن حدث في دِمينغ، وهي بلدة صغيرة قرب الحدود الكندية يبلغ عدد سكانها 353 شخصاً فقط. لا تُعرَف دِمينغ بأنها مرتَع للإرهاب؛ فإذا كانت دِمينع معروفة فبكونها مكاناً للتزوّد بالوقود والشراب عند التلال السَّفحية لجبال نورث كاسكيدز.

بالرغم من ذلك، كانت أمينات المكتبة مستعدّات. فقبل عام، درّبت محامية نظام المكتبة في مقاطعة واتكوم آنذاك، ديبورا غاريت، هيئة الموظفين على كيفية التعاطي مع طلبات أجهزة إنفاذ القانون. كانت أمينات المكتبات قد أصبحنَ محاربات للدفاع عن المعلومات في الثمانينات عندما بدأ عملاء الأف بـي آي بالحضور إلى مكتبات الكلّيات، مطالبين بمعرفة الكتب التي ولجها أجانب. في وقت لاحق، تبنّت ثمان وأربعين ولاية قوانين تحمي بطريقة ما سرّية سجلات تَداول الكتب.

وهكذا، عندما حضر عميل الأف بـي آي إلى دِمينغ، رفضت أمينة المكتبة تسليم السجلات، بل وعدت بإبلاغ محاميها بطلب العميل، ورافقته إلى الباب.

عندما تلقّت غاريت الطلب، اتصلت بعميل الأف بـي آي وسألته عما يريد. فقال إن قارئاً اتصل بالوكالة ليُبلغ عن قيام أحدهم بخربشة ملاحظة على هامش الكتاب تقول، "إذا كانت الأعمال التي أقوم بها تُعتبر جريمة، لِيكُنِ التاريخ إذاً شاهداً على أنني مجرم. ارتكاب أعمال عدوانية ضد أميركا هو واجب ديني ونأمل في أن يكافئنا الله".

بعد الحديث، اكتشفت غاريت أن الاقتباس مأخوذ من مقابلة أُجريت مع أسامة بن لادن عام 1998. فأرسلت المقابلة لعميل الأف بـي آي، معتبرةً "أن هذه الخطوة ستضع حدّاً للأمر"، قالت غاريت. ولكن بعد أسابيع قليلة، وصل أمر بنقل سجلات المكتبة كي تطّلع عليها هيئة محلَّفين عليا، إضافةً إلى طلب من أمينات المكتبة بعدم مناقشة الأمر.

كانت مكتبة مقاطعة واتكوم في موقف صعب. فالإذعان للأمر يعني

التخلي عن المبادئ التي تؤمن بها أمينات المكتبة، ومقاومته تنطوي على صعوبة لأن القانون يقتضي الإذعان لأمر هيئة عليا شرعية. لقد تعيّن على المكتبة النضال لأجل تضييق نطاق الأمر. فاقترحت غاريت أن بالإمكان الاعتماد على سابقة جرت عام 1998: وجدت محكمة فيدرالية في العاصمة واشنطن أنه لا يتعيّن على متجر الكتب كراميربوكس وأفتروووردس تسليم سجلات مبيعات كتاب مونيكا لوينسكي بسبب الحماية التي تحظى بها مواد القراءة وفقاً للتعديل الأول.

لقد شعر القيّمون على المكتبة بالقلق. إذا قاوموا وخسروا، سيكون عليهم مواجهة خيار مروِّع: تسليم المعلومات وخيانة مبادئهم أو مواجهة إمكانية قضاء مدة في السجن بسبب رفض الإذعان للأمر. فناقش القيّمون المسألة وقرّروا المواجهة. "كان من المخيف اتخاذ هذا الموقف"، تذكّر أموري بيك، رئيس مجلس إدارة القيّمين على نظام مكتبة مقاطعة واتكوم. "ولكن لم يكن بإمكاننا القيام بأقل من ذلك. لم يكن بإمكاننا القيام بأقل من حماية حق أساسيّ جداً لزبائننا المنتظمين: قدرتهم على القراءة بفُضول بشكل موسَّع وعام، وربما يكون الأمر أكثر خطورة... من المؤكد أن خياراتهم أ ستكون سرّية".

بعد تقديم غاريت طلباً لإلغاء الأمر استناداً إلى التعديل الأول، سحبت الأف بـي آي الأمر. "من وجهة نظري، تُظهر هذه القضية ما يحدث عندما يعرف الناس أن محكمة ستتفحّص أعمالهم"، قالت غاريت التي أصبحت الآن قاضية. "يُبقي هذا الأمر الناس على استقامتهم".

á á á

لم أتوقع من مزوِّديَّ بالإنترنت أن يدافعوا بهذه الجرأة عن مواد القراءة المتوافرة لي.

بالطبع، هم يحاولون حقاً الدفاع عن زبائنهم، ولغوغل مجموعة من المحامين الرائعين. ففي العام 2006، تحدت غوغل طلباً من وزارة العدل للحصول على سجلات بحث جرت لمدة شهرَين، فائزةً بحق تضييق الطلب إلى خمسين ألف عنوان صفحة ويب بدلاً من البلايين المطلوبة. وفي العام 2007، نجحت أمازون في مواجهة أمر حكومي للحصول على هويات أشخاص اشتروا كتباً من بائعِ كتب مستعمَلة عبر موقعه. وطلبت الحكومة إجراء مقابلة مع شُراة الكتاب في إطار التحقيق الذي تُجريه حول احتيال ضريبـي قام به بائع كتب عبر أمازون، ولكن أمازون رفضت تسليم الأسماء. وافقت المحكمة على "أن تخيُّل عملاء فيدراليين يتطفّلون على قوائم قراءة

مواطنين يلتزمون بالقانون أثناء السعي وراء دليل ضد شخص آخر هو سيناريو مُقلق وغير أميركي".

ولكن عندما يتعلق الأمر بالرَّقابة، غالباً ما تخسر شركات الإنترنت في المواجهة لأن القانون ليس في صفها. فليس هناك قوانين خاصة بالإنترنت مساوية لقوانين الخصوصية العامة التي تحمي سجلات تَداول الكتب في المكتبات، وغالباً ما تُرفض مطالبات التعديل الأول بسبب عدم وجود ضرر فعليّ. ولم يتبنَّ معظم التكنولوجيين وجهة النظر التي تصفهم بأنهم مناضلون في سبيل الحرية الفكرية، كما تفعل أمينات المكتبات في غالب الأحيان.

والقانون ذات الصلة الذي يوجّه معظم رَقابة الاتصالات عبر الإنترنت هو قانون خصوصية الاتصالات الإلكترونية العائد للعام 1986 الذي وُضع لاعتماد التقنية الرقمية وسيلةً لتوسيع حماية الاتصالات الهاتفية والبريد العادي. مع ذلك، لم يلحظ القانون في ذلك الوقت أن الأشخاص سيخزّنون مزيداً من المعلومات على أجهزة الكمبيوتر وعلى برامج خدمات كمبيوترية خارج منازلهم. نتيجةً لذلك، يمكن الحصول على اتصالات مخزَّنة، كرسائل بريد إلكتروني وسجلات مواقع الأجهزة المحمولة، من الحكومة في غالب الأحيان بدون مذكرة تفتيش. فالقانون يفرض على الحكومة التأكيد على أن البيانات "ذات صلة وهامة" لأجل التحقيق.

لذلك، إن قيام أجهزة إنفاذ القانون بقراءة رسائل البريد الإلكتروني للأشخاص بطريقة قانونية هو أسهل من فتح رسائلهم البريدية. لا يقتصر الأمر على ذلك فقط، بل غالباً ما تُحكِم المحاكم إغلاق الأوامر الصادرة عنها والمتعلقة بالرَّقابة الإلكترونية كي لا يُبلَّغ المستخدمون أبداً بإجراء بحث. بالنتيجة، توضع العراقيل أمام بوّابـي بياناتنا أثناء نضالهم لحماية زبائنهم. ففي العام 2012، قدّمت مايكروسوفت بيانات عن زبائنها لـ83 بالمئة من الطلبات المقدَّمة من قِبَل أجهزة إنفاذ القانون. في ذلك العام نفسه، سلّمت غوغل بيانات عن مستخدميها في نحو ثلثَي القضايا التي طُلبت فيها معلومات.

لقد انضمت شركات الإنترنت الرائدة، بما فيها غوغل وأبل وفيسبوك، إلى ائتلاف يحثّ على تعديل قانون الاتصالات الإلكترونية بحيث يفرض استصدار مذكرات تفتيش للحصول على رسائل البريد الإلكتروني وعلى سجلات مواقع الهواتف المحمولة. ولكن مساعيها لإصلاح القانون لم تتكلل بالنجاح.

لم تنتهِ الأمثلة القليلة التي بلغتنا عن مواجهة الشركاتِ الرَّقابةَ

الحكومية بشكل جيد. تأمّلوا بحالتَين - مزوِّد صغير بالإنترنت، Sonic.net ، وعملاق الإنترنت ياهو!. ففي العام 2011، أعلنت Sonic.net أنها واجهت أمراً سرّيّاً صادراً عن المحكمة - وخسرت المواجهة - يقضي بتسليم عناوين البريد الإلكتروني لأشخاص راسلوا لمدة عامَين متطوّعاً في ويكيليكس، يدعى يعقوب أبلبوم. كان تحدّي الأمر "مُكلّفاً، ولكننا شعرنا بأننا فعلنا الصواب"، قال المدير التنفيذي في سونيك، داين جاسبر. بمكالمتي عن الموضوع، تحدّى جاسبر أمر الكتمان الصادر عن المحكمة الذي يمنعه من مناقشة طلب الحكومة. (قال جاسبر في وقت لاحق إنه لم يكن يعلم بأن أمر الكتمان ما يزال ساري المفعول عندما تحدّث إليّ).

أما بالنسبة إلى ياهو!، فقد رفضت محكمة الرَّقابة الاستخباراتية الخارجية عام 2008 اعتراضها على أمر غير مُرفَق بمذكرة يقضي بتسليم المحكمة بيانات خاصة بمستخدمين. جادلت ياهو!، قائلةً إن طلبات الحكومة الواسعة النطاق غير دستورية، ولكن المحكمة حكمت بأن الشركة لم تُثبت إلحاقَ الرَّقابةِ الضررَ بأي شخص: "بالرغم من عرض الملتمس للفظائع، لم يقدِّم أي دليل على ضرر فعلي، أو أي احتمال لحدوث خطأ بالغ، أو أية إمكانية لإساءة الاستعمال في الظروف المحيطة بالحالة".

هناك العديد من الحالات الإضافية، ولكنها تحمل الطابع نفسه: غالباً ما تكون أيدي شركات الإنترنت مقيَّدة عندما يتعلق الأمر بالرَّقابة.

á á á

لا أكره غوغل.

في الواقع، حاولت غوغل جاهدةً أن تكون شفّافة في شأن الرَّقابة. إنها أول شركة إنترنت كبيرة تبدأ بالإبلاغ علانيةً عن عدد الطلبات التي تلقّتها من أجهزة إنفاذ القانون. كانت ناشطة في الائتلاف الذي يحثّ على إصلاح قانون خصوصية الاتصالات الإلكترونية. وتستأنف غوغل أمر الكِتمان الصادر عن الحكومة الذي يمنعها من الكشف عن عدد الطلبات التي تتلقّاها من محكمة الرَّقابة الاستخباراتية الخارجية.

ولكن غوغل أساءت تكراراً إلى ثقة المستخدمين. ففي العام 2010، أطلقت غوغل شبكة اجتماعية تدعى باز (Buzz) تُدرج على الفور أشخاصاً بأنهم "أتباع" أشخاص يوجهون لهم تكراراً رسائل بريد إلكتروني أو يتسامرون عبر بريد غوغل الإلكتروني. فالمستخدمون الذين يضغطون على زر "يا عزيزي (يا عزيزتي)! تحقَّق (تحقّقي) من باز"، لا يبلَّغون بالشكل الملائم بنشر هوية المقرَّبين إليهم الذين يتواصلون معهم عبر بريد غوغل الإلكتروني.

ووافقت غوغل في وقت لاحق على إيجاد تسوية للتُّهم الموجَّهة من قِبَل لجنة التجارة الفيدرالية بأن باز مخادعة، ودفعت 8,5 مليون دولار كتسوية لدعوى قضائية جماعية مقدَّمة ضد باز. وفي العام 2012، نشرتُ وزملائي خبر قيام غوغل بتجاهل إعدادات الخصوصية في متصفّح سافاري الذي يستعين به ملايين مستخدمي آي فون ومستخدمين آخرين لمنتجات أبل، معتمِدةً شيفرة كومبيوترية خاصة كي تخدع برامجهم المتصفّحة وتتمكن غوغل من تتبّعها. في وقت لاحق من ذلك العام، وافقت غوغل على دفع مبلغ 22,5 مليون دولار كتسوية للتُّهم الموجَّهة من قِبل لجنة التجارة الفيدرالية بأن تحايل أبل انتهك شروط التسوية التي أجرتها في شأن باز من غوغل. في ذلك الوقت، كانت التسوية البالغة 22,5 مليون دولار أكبر جزاء مدني فرضته لجنة التجارة الفيدرالية. وفي العام 2013، وافقت غوغل على دفع مبلغ 7 ملايين دولار كتسوية مع ثمانية وثلاثين مدّعٍ عام من ثمانٍ وثلاثين ولاية ادّعت انتهاك غوغل خصوصية الناس عندما جمعت سياراتها ستريت فيو بشكل غير متعمَّد معلومات شخصية من شبكات واي - فاي.

لديّ أيضاً كثير من البيانات المخزَّنة لدى غوغل. لقد كشف تدقيقي عن قيام غوغل بتخزين كل أبحاثي التي أجريتها منذ العام 2006، وحددت هوية 2,192 شخصاً كنت قد تواصلت معهم عبر البريد الإلكتروني في ذلك الوقت. فنظراً لقوانين الخصوصية القديمة العهد، لم أتوقع احتفاظ الشركة بسرّية كل تلك البيانات. كنت بحاجة إلى ممارسة حِمية في شأن بيانات غوغل.

وشرعتُ بالكفّ عن إجراء أبحاث عبر غوغل.

لقد شعرت بالانـزعاج من التغيير الذي طال سياسة الخصوصية المتّبَعة من قِبَل غوغل، والمُعلَن عنها عام 2012، والتي تسمح لغوغل بدمج معلومات من مواقع خدمات متنوّعة، مثلاً، مستخدِمةً معلومات عن أبحاثي لتُريني إعلانات معدَّلة وفقاً للطلب على بريد غوغل الإلكتروني. لا تمحو غوغل أيضاً السجل التاريخي للبحث المرتبط بحساباتي ما لم أمحُه بنفسي. وإذا أجريتُ بحثاً من جهاز كمبيوتر لم أتسجّل من خلاله في حساب لغوغل، فهو سيزيل بعض العناصر التعريفية من البيانات بعد تسعة أشهر. نظرياً، يعني ذلك أن باستطاعة الحكومة أن تطلب من غوغل كل أبحاثي منذ العام 2006. لم يتم الكشف عن طلبات مماثلة، ولكن توافر السجل التاريخي يبدو كدعوة مفتوحة لرِحلات بحث.

وأبحاثي هي من بين المعلومات الأكثر حساسية بالنسبة إليّ. فإذا كنت أُنعم النظر لشراء هاتف محمول مُسبَق الدَّفع، تكون كل أبحاثي عن هذا النوع من الهواتف. وإذا كنت أبحث عن مقالة حول تكنولوجيا تمييز الوجوه، تكون كل أبحاثي عن تكنولوجيا تمييز الوجوه. في الأساس، إن أبحاثي هي تنبّؤ دقيق نوعاً ما بأعمالي المستقبلية.

لاستبدال البحث على غوغل، عثرت على محرّك بحث صغير يدعى داك داك غو (DuckduckGo) لا يتّبع سياسة الاحتفاظ ببيانات. هو لا يخزّن أيّاً من المعلومات التي ينقلها جهاز كمبيوتري أوتوماتيكياً - عنوان بروتوكول الإنترنت وآثار رقمية أخرى. نتيجةً لذلك، لا وسيلة لـداك داك غو كي يربط طلبات بحثي بـي. "عندما تلجون داك داك غو (أو أي موقع على الويب)، يرسل متصفّحكم أوتوماتيكياً معلومات عن جهازكم"، تؤكد سياسة الخصوصية المتّبَعة من قِبَل الشركة. "نظراً إلى إمكانية استخدام هذه المعلومات لربطكم بأبحاثكم، فنحن لا نخزّنها أبداً. إنها ممارسة غير عادية، ولكننا نشعر بأن حماية خصوصيتكم هي خطوة هامة".

حالما ولجتُ داك داك غو أدركت مدى اتكالي على غوغل. فبدون أبحاث غوغل المقترَحة، وذاكرة غوغل الممتازة لِما أبحث عنه في العادة، يتطلب كل بحث عملاً إضافياً من قِبَلي. على سبيل المثال، لا يعرف داك داك غو أنني أُقيم في مدينة نيويورك، لذلك عندما أُدخل خطأً عبارة "متحف التاريخ الطبيعة"، يطرح تلقائياً الاسم الصحيح "متحف التاريخ الطبيعي في لوس أنجلوس". بهدف إجراء مقارنة، تحققت من غوغل: لقد صحّح كتابتي وحزر أنني في نيويورك، مُدرِجاً عبارة "المتحف الأميركي للتاريخ الطبيعي في منهاتن" في رأس قائمة نتائجي.

لقد دفعني افتقار داك داك غو إلى معلومات عني لأكون أكثر ذكاء في أبحاثي. على سبيل المثال، لاحظتُ أنني أصبحت كسولة جداً لدرجة أنني كنت أُدخل عناوين صفحات الويب - مثل CNN.com - في خانة البحث بدلاً من خانة الإبحار، عِلماً أنني كنت أعرف بالتحديد أين سأصل. لذلك، شرعت بإدخال العناوين في المكان الصحيح على متصفّحي.

والأمر الثاني الذي لاحظتُه: كنت أَلِج صفحاتِ ويب عبر غوغل وأزورها بانتظام - مثل مدرستَي صغيرَيّ وجدول أعمال ستوديو اليوغا - بدلاً من اعتماد طريق مختصَرة توجّه متصفّحي نحو هذه الصفحات. وهكذا، بدأتُ باعتماد هذا الأسلوب.

في الواقع، كنت قد اعتدتُ جداً السماح لغوغل بالقيام بعملي لدرجة

انـزعاجي من قيامي بإنهاء إدخال كلمة كاملة دون تولّي غوغل هذه المهمة بالنيابة عني. بدون اقتراحات غوغل، وجدت أنني أقل شروداً بسبب عدم بحثي عن أمور لا أحتاج إليها. لا مزيد من إدخال حرف *a* كي يقترح غوغل " amazon "، ومن ثم تذكُّري فجأةً أنني بحاجة إلى طلب شراء شيء ما من Amazon.com .

بواسطة داك داك غو، أعثر في العادة على ما أريد، عِلماً أنه من الغريب أحياناً أن تجدوا أنفسكم أمام ثلاث نتائج فقط، في حين أنكم ترون "ملايين" النتائج لكل شيء على غوغل.

ولكن هناك بعض الثقوب السوداء في داك داك غو. لقد افتقدتُ بشكل يائس خرائط غوغل ولم أتمكن من العثور على أيّ من الخرائط التي أُحب عبر داك داك غو. وافتقدتُ فقرة غوغل نيوز (News Google).

قبل الذهاب إلى حفلة عشاء يقيمها أحد أصدقائي، أجريت بحثاً لأذكّر نفسي بالترقية التي حصل عليها في جامعة كولومبيا. كانت هناك بعض الأخبار الجديدة عن الأمر، ولكن كل أبحاثي عن اسمه فقط، سري سرينيفاسان، وعن اسمه وكولومبيا معاً، لم تُجدِ نَفعاً. أخيراً، حاولتُ "سري، كولومبيا والأخبار" فظهرت مقالة. كانت الأخبار هناك. لقد تعيّن عليّ إعادة تدريب نفسي على استخدام هيكلية داك داك غو لإجراء أبحاث عن الأخبار.

لقد اتّضح لي أنني كيّفت نفسي مع غوغل. طالما اعتبرت غوغل ورقة نظيفة - بسبب سطحه البَينيّ الأبيض الجميل على الأرجح - ولكنني صغت أسئلتي، في الواقع، للتكيّف مع طريقة إجابة غوغل عن الأسئلة.

وبدأت بتكييف نفسي مع خدمة مختلفة، داك داك غو، التي تعتمد طرقاً مختلفة في الإجابة عن الأسئلة. فالأمر أشبه بعلاقة جديدة: اكتشاف الخصائل الغريبة ونقاط الضعف لدى شريكي الجديد. ولكنني أكيّف نفسي مع شريك لا يملك أية أجندا مخبَّأة لتتبّعي.

لقد تحررتُ من غوغل، ولكن العالم ما يزال يدور في فلَكه، وأتقنتُ العمل على محرّك بحث آخر وما أزال أعثر على المعلومات التي أحتاج إليها. ذكّرني الاختبار برمّته باقتباس من مارك أندريسن، الرجل الذي ابتكر نتسكيب، أول برنامج لتصفّح الويب، عام 1994. "إن انتشار أجهزة الكمبيوتر والإنترنت سيضع المهام في فئتَين"، قال أندريسن في مقابلة أُجريت معه عام 2012. "الأشخاص الذين يقولون لأجهزة الكمبيوتر ما يتعيّن عليها

فعله، والأشخاص الذين يتلقون من أجهزة الكمبيوتر ما يتعيّن عليهم القيام به".

لقد حملني إتقاني لـداك داك غو على الشعور بأنني أمام فرصة أفضل لأكون في فئة الأشخاص الذين يقولون لأجهزة الكمبيوتر ما يتعيّن عليها فعله.

á á á

بعد استخدام داك داك غو طوال أشهر قليلة، بدأتُ أشعر بقليل من عدم الارتياح. من هم هؤلاء الأشخاص الذين أثق بهم؟ ولماذا يكون شعارهم بطة مع ربطة عُنُق على شكل فراشة؟ بدا الأمر غريباً نوعاً ما.

بسبب كُرهي الكبير لممارسات غوغل التعقّبية، طوّرتُ لقطة فوتوغرافية عاطفية عن غوغل كمكان يعجّ بغطرسةٍ مبتهجة لإحدى جامعات آيفي الثماني. لدى غوغل مبادئ ولكن قليل من الارتيابات: تتطلب مواجهة الرَّقابة في الصين شخصاً شجاعاً مصحوباً بدعاية كبيرة، ولكنه يجني مالاً كل يوم من بياناتي الشخصية.

لقد واجهتُ وقتاً عصيباً للحصول على صورة ذهنية مماثلة للمبادئ والارتيابات التي تقف وراء بطة مبتهجة بربطة عُنُق على شكل فراشة.

وهكذا، استقلّيت قطاراً إلى فيلادلفيا لألتقي الأشخاص الذين يقفون وراء البطة. من فيلادلفيا، توجّهتُ بالسيارة مدة عشرين دقيقة إضافية عبر الضواحي المليئة بالأشجار، ومروراً بجانب حَرَم كلية براين مور قبل الوصول إلى مَقصدي، باولي. من السهل رؤية مؤسس داك داك غو، غابرييل وينبرغ، في موقف السيارات - كان أحد الذين تحمل سياراتهم لُصاقات بطة. فباستثناء شعره الخرّوبيّ الكَثّ، بدا كأي مهووس آخر بنظاراته السميكة وقَلَنسوّته. فقفزتُ إلى داخل السيارة وقدنا لمدة دقيقتَين وصولاً إلى مكتبه.

كم كانت دهشتي كبيرة عندما دخلنا موقف سيارات وراء قلعة حجرية ذات أبراج مستديرة ملوَّنة. "تعمل في قلعة؟" قلت.

أجل، بالفعل. فمكاتب داك داك غو في الطابق الثاني، والجدران مزيَّنة ببَطّ. في مكتب وينبرغ أريكة تحمل بُقعاً مستديرة، وقرب طاولته منطقة يلعب فيها صغاره. قال لي إن شركته لم تركّز في الأساس على الخصوصية. أراد فحسب بناء محرّك بحث أفضل. فبعد بيع موقع على الويب للتواصل الاجتماعي التفاعلي يدعى قاعدة بيانات الأسماء (Database Names) بمبلغ 10 ملايين دولار عام 2006، انتقل وزوجته إلى فالي فورج، بنسيلفانيا، كي يكون بجانب عملها في العملاق الصيدلانيّ غلاكسو سميث كلاين.

مليونيراً حديث العهد، اختبر وينبرغ مجموعة من المشاريع. لقد أعدّ الاستوديو التلفزيوني الخاص به، وعمل على شبكة للتواصل الاجتماعي لصالح لاعبـي الغولف، وشرع بالحصول على خدمات ضرورية عبر الإنترنت من مجموعة أشخاص بهدف تحقيق نتائج بحث أفضل. أثناء قيامه بهذا الأمر، بدأ يشعر بانـزعاج متزايد من نتائج بحث توفّرها غوغل مليئة بما يعادل نسخات عدة لرسائل موجَّهة تُغرِق الإنترنت.

لذلك، قرر بناء محرّك بحث أفضل. "أردت العودة إلى أيام غوغل الغابرة عندما كان التركيز على أدواتِ ربطٍ نوعية"، قال لي. لم يقرّر الاهتمام بالخصوصية إلا بعد تقديم النسخة الأولى للموقع لمجتمع التكنولوجيا، وسأل بعض المستخدمين عن سياسات الموقع في ما يتعلق بالخصوصية. "بصدق، لم يسبق لي أن فكرت بالخصوصية حتى ذلك الحين"، قال لي وينبرغ. "لذلك، ألقيت نظرة متفحّصة على خصوصية البحث. كنت أعتقد أن ما يملكه محرك البحث عن أحدهم يبعث على القشعريرة تماماً - يمكن مناقشة البيانات الأكثر حساسية التي قد تمتلكينها عن أحدهم على الإنترنت. فقررت أن مسار العمل الأفضل يتمثل بالابتعاد عن هذا الأمر كلّيّاً - وليس تخزين المعلومات. بعد قيامي بذلك، أدركت أنها أطروحة أساسية من نوع ما بالنسبة إلى الشركة".

عام 2011، تقبّل الخصوصية تماماً، واشترى لوحة إعلانات في سان فرانسيسكو تحمل عبارة، "غوغل تتعقّبكم. نحن لا نتعقّبكم"، وقبل استثماراً من شركة رؤوس أموال استثمارية، هي يونيون سكوير فنتشورز، تراهن على سوق أدوات الخصوصية الناشئ.

حول مائدة تناول شطائر، انضمّ إلينا عدد قليل من المهندسين لمناقشة تحديات بناء محرّك بحث من الصفر. فتحدثنا عن تحديات بناء خرائط أفضل وعن إحباطاتي من نتائج البحث عن الأخبار على محرّك بحثهم. كان من الصعب إبقاء داك داك غو صديقاً للخصوصية. لقد تعيّن على المهندسين بناء العديد من أدواتهم التقنية من الصفر. على سبيل المثال، تعيّن عليهم بناء برنامج تدوين خاص بهم لأن برنامج التدوين المجّاني يتضمّن تكنولوجيا تعقّبية.

"يبدو أنكم تعتبرون استمراركم هدفاً رئيسياً"، قلت لوينبرغ. "عليكم زراعة طعامكم وتخزين أسلحتكم".

أثناء تبادل أطراف الحديث، تفاجأت بمدى جدّيّتهم في معالجة مسألة بناء محرّك بحث أفضل. بطريقة ما، وبوجود أريكة تحمل بُقعاً مستديرة،

وبطّ، وقلعة، وشعر وينبرغ الخرّوبـي، سمحت لنفسي بالتفكير في أن ما يقومون به هو هواية أكثر منه شركة فعلية. ولكنهم بدوا جدّيّين تماماً.

لقد ذكّرني ذلك بالفترة التي كنت فيها مراسلة لدى سان فرانسيسكو كرونيكل في أواخر التسعينات. كنت رافضة لمحرك بحث غوغل الذي هو من نوع جديد. وأذكر قولي لنفسي: كيف يمكن لاتكاله على ترتيب الصفحة بالاستناد إلى آلة أن يكون أفضل من النتائج المرتَّبة يدوياً على محرّك بحثي المفضَّل ألتا فيستا (AltaVista)؟

كنت جالسة على أريكة تحمل بُقعاً مستديرة في ضواحي فيلادلفيا أتساءل عن كيفية تشكيل عدد قليل من الأشخاص يعملون في قلعة تهديداً لمحرّكِ بحث يجني نحو 30 بليون دولار في العام.

ومع ذلك، تبدو بعض أفضل الأفكار في صناعة التكنولوجيا ضرباً من الجنون في بادئ الأمر.

á á á

لم أشأ في الواقع الإقلاع عن استخدام بريد غوغل الإلكتروني. فمعظم أصدقائي المتعقّبين يستخدمونه - لا بل أيضاً أولئك المصابين بالذُّهان الارتيابـي في شأن الخصوصية. فبريد غوغل الإلكتروني يسهّل تشاطر المستندات والتسامر مع مستخدمين آخرين له.

ولكن يصعب تبرير استخدام خدمة بريد إلكتروني أقرّت بقراءة بريدي. بالطبع، تقول غوغل (ولا سبب لنا لعدم تصديقهم) إن البشر لا يقرأون بريدي، بل أجهزة الكمبيوتر فقط التي تمسح بريدي الإلكتروني بحثاً عن كلمات مرور، ومن ثم تُدخل إعلانات بالاستناد إلى كلمات المرور تلك.

ولكن هذا ما تقوله وكالة الأمن القومي أيضاً عن التجسس المحلي. أجل، تغرف أجهزتها الكمبيوترية كل أنواع البيانات الأميركية "عن غير عَمد" في سياق التجسس الخارجي. ولكنها "تخفّض إلى الحد الأدنى" بيانات تتناول مواطنين أميركيين كي لا يراها البشر إلا في بعض الحالات، أثناء إجراء تحقيق استخباراتي، مثلاً، أو إذا كانت البيانات تحتوي على دليل ارتكاب جريمة.

في النهاية، يُطرَح السؤال نفسه المطروح في شأن كل شبكات التعقُّب عبر الإنترنت: هل يساء استعمال البيانات؟ يبدو أن الجواب المقدَّر هو نعم. ففي العام 2010، طردت غوغل مهندساً بسبب تجسّسه على مسامرات مراهقين ومراهقات على بريد غوغل الإلكتروني - وقالت إن مهندساً يُطرد للمرة الثانية بسبب التجسّس على بيانات مستخدمين. في

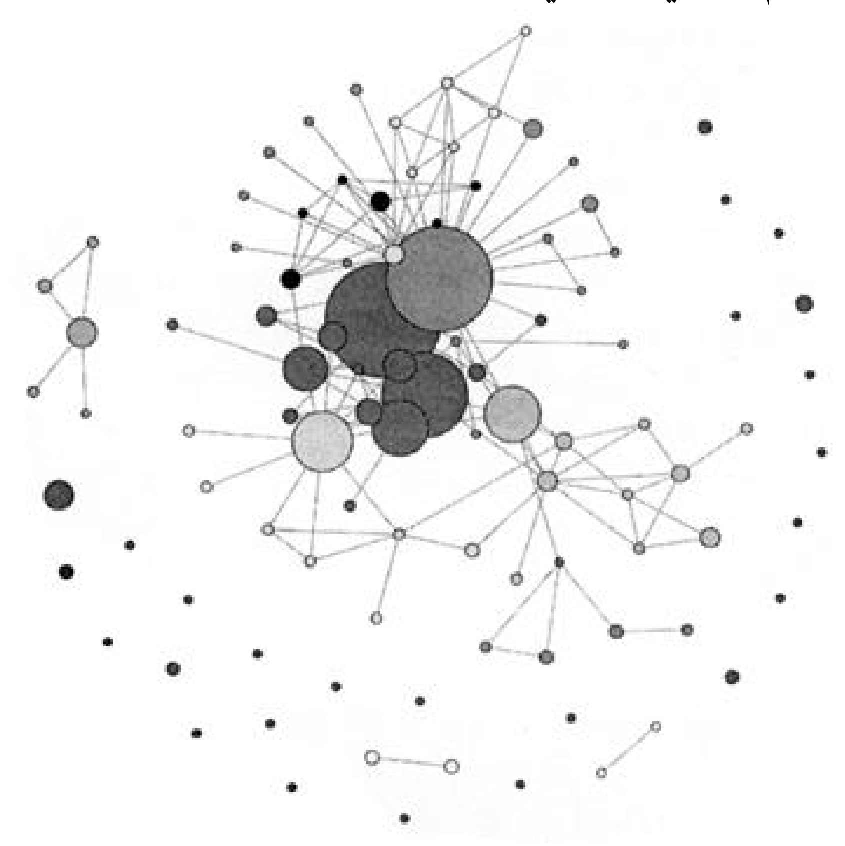
العام 2008، كشف عاملا اعتراضِ بيانات في وكالة الأمن القومي عن تنصّتهما وزملائهما على مئات الاتصالات الهاتفية لأميركيين - بما فيها جنس عبر الهاتف.

مع ذلك، أواصل إرجاء تخلّيَّ عن بريد غوغل الإلكتروني. إنه شديد السهولة، مساعد، ويمكن تفحّصه.

أخيراً، يعود الفضل في إقناعي على البحث عن خدمة بريد إلكتروني جديد إلى مشروع في معهد ماساتشوستس للتكنولوجيا. لقد بنت مجموعة من الباحثين هناك أداة تدعى إيمرشن (Immersion) تسمح للناس بتخيّل ما وراء البيانات في حساباتهم على بريد غوغل الإلكتروني.

من المرعب قليلاً السماح لإيمرشن بولوج حسابي على بريد غوغل الإلكتروني، ولكن المطوِّرين وعدوا بمحو البيانات المكتشَفة. لذلك، اتخذت خطوة جريئة. وبعد دقائق قليلة من الحساب، قدّمت لي إيمرشن رسماً بيانياً جميلاً يُظهر اتصالاتي بأبرز "مشاركيَّ" الـ504 عبر البريد الإلكتروني - أشخاص تبادلت معهم أكثر من ثلاث رسائل عبر البريد الإلكتروني. وفقاً لإيمرشن، كان أبرز "مشارك لي" صديقتي المفضَّلة ويليها زوجي. (سبق لبريد غوغل الإلكتروني أن أبلغني بأن زوجي هو شريكي الأكثر تواتراً عبر البريد الإلكتروني. لست واثقة من أيٍّ من التقريرَين هو التقرير الصائب).

وبدا الرسم البياني لشركائي على هذا النحو:



أوضح الرسم البياني أنني وجهت رسائل عبر البريد الإلكتروني لنحو عشرة أشخاص أكثر من أي مستخدم آخر. لقد ذكّرني الأمر بمدى فرادة شبكة تواصلي الاجتماعية.

منـزعجة، شرعتُ بمحاولة فك ارتباطي ببريد غوغل الإلكتروني.

لقد فكرت لمدة وجيزة في تسيير الجهاز الخادم للبريد الإلكتروني الخاص بـي في المنـزل بعد مصادفة منشورِ مدوَّنةٍ تدعى "وكالة الأمن القومي تختبر بريدك الإلكتروني في غضون ساعتَين". ولكنني تخلّيت عن الفكرة بعد قراءة ثمانية مقاطع من المنشور عندما قال الكاتب، "سوف أفترض أنكم تسيّرون دبيان ويزي (Wheezy Debian)". من الواضح أنه عمل تقنيّ جداً بالنسبة إليّ.

لذلك، بحثت في الأرجاء عن خدمات بريد إلكتروني تحمي الخصوصية، وثَبُت وجود العشرات منها - مع أسماء مثل هاشميل (Hushmail)، نيوميل (Neomail)، وكاونترميل (CounterMail) - خدمة بريد إلكتروني مدفوعة تُجري اختبار بِركة الوحل - ولكن تعيّن عليّ استبعادها لأنها قائمة في السويد. فكوني مواطنة أميركية، يحمي القانون بريدي الإلكتروني؛ لقد "خفّضت وكالة الأمن القومي إلى الحد الأدنى" تجسسها على رسائل المواطنين الأميركيين الموجَّهة عبر البريد الإلكتروني. ولكن إذا اعتقدت الوكالة أنني أجنبية، يقلّ عدد القيود إلى حد كبير.

لقد تركني ذلك مع عدد قليل من الخيارات القائمة في الولايات المتحدة، بما فيها لافابيت (Lavabit)، وهي خدمة في تكساس استخدمها إدوارد سنودن كما يبدو، ورايزأب (Riseup)، وهي خدمة تسيّرها جماعة في سياتل. بعد دراسة سياساتهم المتعلقة بالخصوصية، اعتبرت أن رايزأب هي أكثر إرضاءً بقليل. فكلاهما يخزّنان أقل قدر من المعلومات تتناول المستخدمين، ويُجريان اختبار بِركة الوحل. ولكن رايزأب تحصل على المواقع أيضاً من عناوين البريد الإلكتروني، في حين أن لافابيت تقول إنها تحفظ الموقع في عناوين البريد الإلكتروني كي تتمكن أجهزة إنفاذ القانون من استخدامه.

لم يكن الانضمام إلى رايزأب سهلاً. إنه مجّاني ولكنني كنت بحاجة إلى "دعوة" من قِبَل أحد الأعضاء. لحسن الحظ، تمكنت من تدبّر دعوة من خلال كريستوفر سوغويان، وهو خبير تكنولوجي في الاتحاد الأميركي للحريات المدنية الذي يُصادَف أيضاً أنه أحد الأشخاص الأكثر معاناة من الذُّهان الارتيابـي الذين أعرفهم (أقول ذلك على سبيل الإطراء).

مسلَّحةً بالدعوة، شرعتُ بعملية التسجّل. ولكن سرعان ما اصطدمت بالعقد الاجتماعي الذي طُلب مني توقيعه:

نطلب منكم عدم استخدام خدمات riseup.net لتأييد أيٍّ من الأمور التالية:

- دعم الرأسمالية، الهيمنة، أو الهرمية.
- الفكرة المتمثلة بأن الظلم الطبقي يحلّ مكان الظلم العِرقي أو الظلم الذي يفرّق بين الجنسَين.
- استراتيجية طليعية للثورة.
- التحكم بالشعوب.

إذا كنتم غير موافقين على ذلك، إذاً riseup.net ليس لكم.

لا يمكن الاعتراض على معظم ما جاء في العقد. لم أكن أخطط لاستخدام رايزأب كي أحرّض على الثورة، أو أحثّ على التحكم بالشعوب، أو أشارك في مناقشة جانبَي مسألة الطبقة الاجتماعية إزاء العِرق/الجنس، أو أؤيّد الهيمنة أو الهرمية.

ولكن التنصل من "تأييد الرأسمالية" صعب. فبالرغم من كل شيء، كنت أعمل لصالح وول ستريت جورنال - صحيفة روّجت ذات مرة لنفسها بشعار "مغامرات في الرأسمالية". ولكنني قلت في نفسي إن عملي كمراسلة هو بمثابة حراسة للرأسمالية وليس تأييداً للرأسمالية بدون تحفّظ. ربما كنت أَعرب الكلمات، ولكنني اعتبرت أن باستطاعتي الموافقة على عقد رايزأب الاجتماعي.

لم أنتهِ بعد. لقد تعيّن عليّ إيجاد طريقة لإدارة بريدي الإلكتروني من جهازي الكمبيوتري بدلاً من الويب. يسمح رايزأب للمستخدمين بتخزين مقدار قليل من البيانات فقط على جهازها الخادم، مما يُبقي الكلفة منخفضة، ويعني، وهو أمر أكثر أهمية، أن البيانات التي تحصل عليها الحكومة من رايزأب تكون أقل. بالطبع، يَعد رايزأب بأنه "سيواجه بفعالية" أية محاولة للحصول على بيانات المستخدمين - ولكنها تكون على الدوام مواجهة أسهل إذا لم تكن هناك بيانات تثير مواجهة.

مع أو بدون كوتات رايزأب، كان يُفترض بـي تخزين رسائل بريدي الإلكتروني القديمة على جهازي الكمبيوتري بدلاً من تخزينها في مصادر وأنظمة بريد غوغل الإلكتروني. يسمح قانون خصوصية الاتصالات الإلكترونية للحكومة بالحصول على رسائل البريد الإلكتروني المخزَّنة لدى طرف ثالث

بعد 180 يوماً بدون مذكرة، لذلك فتخزين بريد قديم في أي مكان خارج المنـزل هو، لسوء الحظ، دعوة لشبكات التعقُّب الحكومية.

وبحثتُ عن برنامج بريد إلكتروني صديق للخصوصية. كان أفضلَ خيار مشروعٌ مجاني مكشوف المصدر، ثاندربيرد (Thunderbird)، يدعم رسائل البريد الإلكتروني المشفَّرة. ولكن الداعم الأكبر لثاندربيرد، موزيلا، سحب دعمه المالي عام 2012.

ملتزمةً بمبدأي التوجيهي المتمثل بـ"الدفع لقاء الأداء"، اشتريت نسخة مدفوعة من ثاندربيرد، تدعى بوست بوكس (Postbox). (وهبتُها أيضاً لجماعة رايزأب أَمَلاً في إبقاء خدمة البريد الإلكتروني حيّة). لقد وضعت كل بريدي الإلكتروني الموجَّه عبر غوغل في بوست بوكس وأعددت رايزأب للعمل مع بوست بوكس. عندما جعلتُه يعمل، انتابني شعور بالحرية مثير للدهشة. فجأةً، بات بإمكاني التنقل بين موفّري البريد الإلكتروني، وتلقّي بريد إلكتروني في خدمة غوغل والإجابة من حساب رايزأب.

من الغريب أنني كنت مترددة في بادئ الأمر باستخدام حساب رايزأب. كنت قلقة من عدم رغبة الناس في تلقي رسائل بريد إلكتروني من جماعة مناهضة للرأسمالية. لذلك، وجّهتُ رسائل بريد إلكتروني لعدد قليل من الأشخاص الذين قد يكونون الأكثر قلقاً - أشخاص في مناصب حكومية رفيعة ومدراء تنفيذيون رفيعو المستوى - وسألتهم عما إذا كانوا يمانعون توجيهي رسائلَ بريد إلكتروني لهم من عنوانِ جماعة مناهضة للنظام.

تراوحت الإجابات بين "هاه؟" و"ماذا؟" لم يكن أحد يُبالي، كما يبدو. وخطر ببالي أنني عندما انضممت إلى بريد غوغل الإلكتروني، لم أطلب من أحد "الموافقة" على قيام غوغل بمسح بريده أو بريدها الإلكتروني.

(تجدر الإشارة إلى أن عدداً قليلاً ممن لا يستخدمون بريد غوغل الإلكتروني انضموا إلى دعوى قضائية جماعية ضد غوغل بسبب هذه المسألة بالذات، انطلاقاً من فكرة أن غوغل تنتهك قانون التنصت عندما تمسح رسائل البريد الإلكتروني التي يوجهونها لمستخدمي بريد غوغل الإلكتروني. تُجادل غوغل، قائلةً إن هناك قَبول ضِمنيّ، "تماماً كما أنه لا يمكن لموجِّهِ رسالة لزميلٍ في العمل أن يتفاجأ من فتح مساعدِ المتلقّي الرسالةَ". لست واثقة من تصديقي تلك الحجة. بالرغم من كل شيء، أسأل على الدوام قبل فتح بريد زوجي).

لقد أدركت أنني أقدّم لمن أتواصل معهم عبر البريد الإلكتروني صنيعاً بانتقالي إلى خدمة لن تقوم بمسح رسائلي. وكففتُ عن السؤال وشرعت

باستخدام رايزأب لكل اتصالاتي المهنية.

ولكنني لم أسحب سِدادة بريد غوغل الإلكتروني بالكامل. لقد قررت الاحتفاظ به، تماماً كما احتفظت بحسابـي على أيه أو أل طوال كل تلك السنوات. فـأيه أو أل انتقلت ببطء إلى داخل بريدي الإلكتروني لأجل التسوّق عبر الإنترنت. وقررت الاحتفاظ ببريد غوغل الإلكتروني واستخدامه فقط للتعاطي مع بريد "أمي" الإلكتروني - تحديد مواعيد اللعب لصغيرَيّ، تسجيل صغيرَيّ في المخيّم، والتواصل مع المدرسة عبر مستندات غوغل المشترَكة الحتميّة.

وكخطوة أخيرة، وضعت كل مستندات غوغل المشترَكة على قرصي الصلب. الآن، نادراً ما أكون بحاجة إلى تسجيل دخولي إلى موقع غوغل على الويب. وعندما أقرر التسلل لإجراء بحث عرَضيّ على غوغل، لا يكون البحث مرتبطاً بهويّتي إذا لم أسجّل دخولي إلى غوغل. (عِلماً أن الأبحاث تبقى مرتبطة ببروتوكول الإنترنت الخاص بجهازي ما لم أقنّع عنواني من خلال استخدام برنامج لإخفاء الهوية).

لقد شعرتُ كما لو أنني تسلّقت قمة إفريست تكنولوجية من نوع ما. أنا أتحكم ببريدي الإلكتروني الذي لم يَعد يتحكم بـي.

á á á

كانت غبطتي قصيرة الأمد.

ففي آب/أغسطس 2013، أُغلقت خدمة البريد الإلكتروني لإدوارد سنودن، لافابيت، بشكل مفاجئ. وكتب المؤسس، لادار لفيسون، إنه أغلق الخدمة بدلاً من أن يصبح "مشاركاً في جرائم ضد الشعب الأميركي". قال لفيسون إنه يخطط لنقل معركته إلى محكمة الاستئناف للدائرة الرابعة، مُلمِحاً إلى خوضه معركة من قَبل - وخسارته - في محكمة أدنى مرتبة.

كما في العديد من قضايا الرَّقابة الإلكترونية، تلقّى لفيسون أمرَ كِتمان يمنعه من مناقشة الطلب. ولكن بعد فضّ الخَتم عن بعض المستندات في القضية، كشف لفيسون عن تلقّي طلب بتسليم مفاتيح التشفير التي تُزيل سرّية كل اتصالات مستخدميه. بمعنى آخر، طُلب منه نقض اختبار بِركة الوحل. "يوازي ذلك الطلبَ من كوكا - كولا تسليم صيغتها السرّية"، قال لفيسون.

سبق لهذا النوع من الأمور أن حدث لخدمة بريد إلكتروني مشفَّر. ففي العام 2007، أوحت هاشميل، وهي خدمة بريد إلكتروني مهتمة بالخصوصية، بأنها ربما تكون قد تلقّت أمراً من المحكمة لتثبيت برنامج

يمكنه اعتراض كلمة مرور الزبون عندما يسجّل المستخدم دخوله إلى الخدمة، ممكّناً الحكومة من فك شيفرة بيانات المستخدم.

لقد تمكنت من فهم سبب قرار لفيسون الإغلاق حفاظاً على المبدأ بدلاً من خرق خصوصية مستخدميه. ولكنني لم أتمالك نفسي أيضاً من الشفقة على أربعمئة ألف شخص فقدوا حسابات بريدهم الإلاكتروني دون أي إشعار. "سنوات من حسابات البريد الإلكتروني، والبريد المدَّخَر، والتفاصيل الهامة، زالت بدون إشعار. إنه عار على الشركة"، كتب مستخدم على صفحة لافابيت على فيسبوك. "إنه أمر مروِّع... شكراً لإفسادكم حياتي"، علّق مستخدم آخر.

كان بالإمكان أن أكون أنا. فقد كانت لافابيت خياري الثاني كخدمة بريد إلكتروني.

بعد إغلاق لافابيت، أغلقت شركة أخرى تحمي الخصوصية، هي سايلنت سيركل، خدمةَ بريدها الإلكتروني بشكل مفاجئ. قالت الشركة إنها لم تتلقَّ بعد أية طلبات حكومية، ولكنها أرادت التصرف قبل وصول أية طلبات. "نرى الكتابة على الجدار، وقررنا أنه من الافضل لنا إغلاق سايلنت ميل (Mail Silent) الآن"، كتبت الشركة.

فجأةً، أصبحت رايزأب من بين آخر خدمات البريد الإلكتروني الحامية للخصوصية التي ما تزال مستمرة بالعمل. لقد نشرت جماعة رايزأب رسالة على فيسبوك تُطمئن المستخدِمين إلى أنها ستواجه أية محاولات للرَّقابة الحكومية، وأنها تعمل لإنشاء "بنية تحتية راديكالية جديدة" تحمي البريد الإلكتروني للمستخدمين بشكل أفضل. مع ذلك، لم تكن هذه الرسالة مطمئنة بالكامل.

"نفضّل سحب السِّدادة بدلاً من الاستسلام لرَقابة قمعية من قِبَل حكومتنا، أو أية حكومة"، كتب قادة الجماعة. وذكّروا المستخدمين بإجراء نسخات لبريدهم الإلكتروني.

وبتحققي للمرة الثالثة من إجراء نسخات عن بريدي الإلكتروني على قرصي الصلب وداخل خدمة سحابتي (مصادر وأنظمة كمبيوترية متوافرة تحت الطلب - Cloud computing) المشفَّرة، فكّرتُ في مدى السُّخف الذي غدت عليه رحلتي إلى الخصوصية.

كنت أدّخر كل بياناتي تحسّباً لأحداث عظيمة. والأكثر غرابة أن الأحداث العظيمة تبدو وشيكة. كنت أتحوّل إلى ناجية ببياناتي.

الفصل التاسع
تقديم معلومات متعلقة بآيدا

كانت آيدا تاربيل صحفية استقصائية كشفت عن إساءات ستاندارد أويل كومباني عند منقلَب القرن العشرين. هي أيضاً ذاتي الثانية.

كان ابتكار هوية زائفة جزءاً أساسياً من استراتيجيتي لتلويث البيانات. ففي حالات عدم تمكّني من تجنّب شبكة تعقُّب عبر الإنترنت، عندما أشتري أشياءً، في الغالب، أو أسجّل دخولي إلى مواقع على الويب، أحاول تقديم معلومات متعلقة بآيدا لشبكة التعقُّب بدلاً من تقديم معلومات متعلّقة بـي. بالرغم من كل شيء، لا سبب كي يعرف كلُّ موقع على الويب، يستدعي تسجّلي، اسميَ الحقيقي.

بالطبع، سيكون خصم عازم قادراً على الأرجح على وصل النقاط بين آيدا وبيني. ولكنني لم أكن أبحث عن الكمال؛ أردت فحسب إرغام المتعقِّبين على بذل بعض الجهد لتعقّبـي بصفة خاصة، بدلاً من جرف بيانات عني بدون عناء.

لقد اخترت آيدا لأنها جزء من جيلِ صحافيين وصحافيات أَكنّ لهم ولهنّ الإعجاب. معروفون بأنهم "كاشفو الفساد"، يكشف الصحافيون الاستقصائيون، مثل آيدا تاربيل وأبتون سينكلير، عن النواحي غير المنيعة في الثورة الصناعية، بدءاً بأسعار مجموعات الشركات الاحتكارية وصولاً إلى ظروف العمل في المسالخ. لقد أدّى عملهم إلى قوانين كبحت أسوأ تجاوزات العصر.

أعتقد أننا في الوقت الحاضر عند نقطة تحوّل مماثلة. فبتحوّل أمّتنا إلى اقتصاد المعلومات، هناك عدد قليل من القوانين التي تضبط عمالقة الصناعة المزدهرة وعدداً قليلاً من المؤسسات الحكومية، أو تلك التي لا تبتغي الربح، من خلال الفهم التقني بهدف تنظيم اقتصاد المعلومات. وهكذا، شرع كاشفو الفساد - صحافيون استقصائيون ومعترضون ذوو ضمائر مثل إدوارد سنودن - بالكشف عن النواحي غير المنيعة في الثورة الصناعية. آمل في أن نكون قادرين، متى رأينا الإساءات بوضوح، على كبح جماح تجاوزات عصر المعلومات.

ولكنني لم أكن واثقة من كيفية ابتكار هوية لآيدا عبر الإنترنت. كنت قد اتخذت قراراً بعدم ابتكار رخصة سَوق زائفة. ولكن كل شيء آخر -

عناوين بريد إلكتروني زائفة، أرقام هواتف، عناوين بريدية - هو خدعة عادلة.

وسرعان ما وجدت نفسي على منحدر أكاذيب زَلِق.

á á á

لقد بدأت بشكل متواضع: أعددت حساب بريد غوغل إلكتروني لآيدا، مما يعني ابتكار تاريخ مولد ورمز بريدي لها. وارتأيتُ أنها مقيمة في بركلي، كاليفورنيا، ومولودة عام 1966.

بعد ذلك، شرعتُ بتسجيل حجوزات باسم آيدا تاربيل في عدد قليل من المطاعم. تمثّلت المشكلة في عدم امتلاك آيدا هاتفاً محمولاً - وغالباً ما تسألني المطاعم عن رقم هاتف عندما أقوم بالحجز.

تمكنت من إقناع بعض المطاعم بتسجيل حجز باسمي بدون رقم هاتف، واعدةً إيّاهم بالاتصال بهم لتأكيد الحجز. فوافقوا، وغالباً ما يحتفظون بالحجز إذا نسيتُ الاتصال بهم.

ولكنني وجدت أنني أجد صعوبة في الكذب: يحمرّ وجهي قليلاً كلما تعيّن عليّ قول اسم آيدا. وسرعان ما أدركتُ أن آيدا بحاجة إلى حساب أوبن تيبل (OpenTable) - للحجز عبر الإنترنت - كي لا أكذب في شأن الهاتف.

ولكن عندما حاولت الاشتراك في أوبن تيبل، سألني عن رقم هاتف محمول. كنت أعرف أنه يُفترض بي إدخال رقم هاتف عشوائي مثل 212-555-1212، ولكنني لم أتمكن من القيام بذلك بطريقة ما. وخرجتُ من شاشة الاشتراك.

لقد واجهتُ المشكلة نفسها مع كلمات المرور. لم تكن التكنولوجيا المشكلة، بل طبعي.

á á á

أنا كاذبة رهيبة.

أشعر بالحرَج ولا أُقيم اتصالاً بصرياً، ويحمرّ وجهي؛ أم أقهقه. أنا كاذبة رهيبة لدرجة قيام زميلة لي ذات مرة بأخذي جانباً والقول لي إنه لا يُفترض بي أبداً محاولة الكذب لأنني لا أجيد القيام بالأمر بالشكل الصحيح.

طالما اعتقدت بأنه من الأسهل الكذب عبر الإنترنت. فبعض الدراسات تُظهر أن تجنّب الإشارات الجسدية التي ترافق الأكاذيب يمكن أن تجعل الكذب عبر الإنترنت أكثر سهولة. ولكنني لم أعد أجد العملية أكثر سهولة

عبر الإنترنت. لم أفهم سبب ذلك حتى وقعتُ على بحث جيف هانكوك، وهو عالِم نفس في جامعة كورنيل يدرس التضليل عبر الإنترنت.

ففي دراسة تعود للعام 2012، طلب هانكوك من 119 طالب جامعي ابتكار خلاصة تقليدية أو نِبذة عامة عن LinkedIn ، وحلّل من ثم صِدقية النتائج. فالطلاب الذين ابتكروا خلاصات تقليدية بالغوا بالمعلومات المرتبطة بخبراتهم العملية السابقة أكثر من أولئك الذين ابتكروا نِبذات عامة. ولكن الفريقَين كذبا في شأن هواياتهم واهتماماتهم. على وجه العموم، قال هانكوك إن "خلاصات LinkedIn كانت أكثر صدقاً في شأن الأمور التي تهمّ الموظفين، كمسؤولياتكم أو مهاراتكم في العمل السابق".

في دراسة سابقة، قارن هانكوك الطول الحقيقي لقامة الأشخاص، ووزنهم، وعمرهم، مع ما ذكروه في نِبذة مواعَدة عبر الإنترنت. فمعظم الناس يبالغون، ولكن بمقدار قليل فقط. ومعظم الرجال يكذبون في شأن طول قامتهم، قال هانكوك. "في الواقع، كذبوا في شأن طول قامتهم بنحو تسعة أعشار البوصة، وهو ما يُعرف بلغة المختبر بـموجَز مقتضَب".

يعتقد هانكوك أن باستطاعة الناس أن يكونوا أكثر صدقاً عبر الإنترنت منه شخصياً إذا اعتقدوا أنهم سيحمَّلون مسؤولية ما يكتبون. وفي دراسات أخرى، وجد أن الأكاذيب تزداد عندما تكون مدة الحديث أقصر - سواءً كانت مسامَرة عبر الإنترنت أو حديثاً وجهاً لوجه. وتزداد الصدقية عندما يعرف الأشخاص بعضهم البعض في الواقع. باختصار، يظنّ هانكوك أنه من الصعب الكذب عندما تبتكرون سجلاً دائماً وتعرفون أنكم ستحمَّلون مسؤولية المعلومات الواردة فيه. بعد التدقيق ببياناتي، أُدرك تماماً أن كل ما أقوم به يسجَّل. لذلك، من المنطقي أن أمرّ بوقت عصيب عندما أكذب عبر الإنترنت.

بعد أن فهمت الوضع، واجهتُ خياراً صعباً: هل من الأخلاقي أن أحاول التغلّب على كرهي الشديد من خلال الكذب؟ للإجابة عن هذا السؤال، وجدت نفسي برِفقة فلاسفة. فإحدى وجهات النظر الأكثر تطرّفاً تعود للفيلسوف الألماني إيمانويل كانت، في القرن الثامن عشر، الذي اعتبر الكذب أمراً خاطئاً على الدوام - حتى ولو ظهر قاتل عند بابكم بحثاً عن ضحية بريئة.

كوالدة، وجدت أنه من السهل طرح وجهة نظر كانت المتطرفة جانباً. فأية والدة تعرف أنه يتعيّن عليكم الكذب على أبنائكم أحياناً. عندما كنا في غرفة الطوارئ بسبب شقّ ابني بنانته في حادث، لم أخبره بالحقيقة -

ألا وهي أن الطبيب الجرّاح عالق في عاصفة ثلجية مُعمِية وليس واثقاً من تمكّنه من الحضور إلى المستشفى في الوقت المحدد لتقطيب الجرح. وقلت له إن كل شيء سيكون بخير. (وأجل، تمكن جرّاح التجميل من تقطيب إصبع ابني - ولكن الأمر تطلّبه نحو خمس ساعات لبلوغ المستشفى).

لذلك، أعتبر أن بعض الأكاذيب مقبولة. ولكن أيٌّ منها؟ ووجدت نفسي منجذبة إلى "اختبار الإعلان جَهاراً" الذي وصفته كاتبة وفيلسوفة هارفارد سيسيلا بوك: "أيٌّ من الأكاذيب، إذا وُجدت، تنجو من دعوة أشخاص منطقيين لتبريرها؟"

في ما يلي بعض الأسئلة التي تطرحها:

1 هل هناك بدائل صادقة لكذبتكم؟

- ما هو التبرير الأخلاقي لإطلاق كِذبة؟
- ما العلاقة القائمة بينكم وبين الشخص الذي تكذبون عليه؟
- ما هي الحسنات والسيئات التي ستتسبب بها كذبتكم؟
- ماذا يحدث إذا كذب كل من هو في وضعكم؟

هنا، شعرت بأنني على أرض صلبة نوعاً ما. كنت أخطط لاستخدام هويّتي الزائفة للقيام بمعاملات تجارية مع شركات أعتقد أنها تطلب مني معلومات أكثر مما هو ضروري لإتمام الصفقة.

وبإمكاني التوجه إلى منصة صحف، والدفع نَقداً، وشراء نسخة صحيفة دون الكشف عن اسمي. ولكن كل موقع صحيفة على الويب يريد معرفة كل شيء عن هويّتي - حتى ولو لأجْل تسجّل "مجّاني". بشكل مماثل، اعتدتُ الذهاب إلى متجر الكتب المحلّي وشراء كتب نَقداً. والآن، كل متاجر الكتب تضمحلّ، وبات أمازون متجر كتبـي المحلي. ولكن لماذا يكون أمازون بحاجة إلى شيء آخر غير مالي؟ هل المطاعم حيث أُجري حجوزاتي بحاجة حقاً إلى شيء آخر غير مالي؟

من الواضح أن بعض هذه المعلومات، إذا لم تكن كلها، تُستخدم ضدي. تأمّلوا بمثالَين.

في العام 2012، تبنّى الاتحاد الدولي للنقل الجوّي قواعد جديدة تسمح لشركات النقل الجوي بتقديم أسعار مختلفة لزبائن مختلفين. وحذّر مجلس تحرير نيويورك تايمز من احتمال استخدام النموذج التسعيري الجديد لتقديم أسعار أكثر ارتفاعاً لأشخاص يحاولون التسوّق دون الكشف عن أسمائهم، ولأشخاص يبدون قادرين على دفع المزيد.

في العام 2013، قالت بلو كروس بلو شيلد في كارولاينا الشمالية إنها

بدأت بشراء معلومات من وسطاء بيانات تتناول عادات الإنفاق لأكثر من ثلاثة ملايين شخص. وقال المؤمّن إن باستطاعة المعلومات الإشارة إلى الأشخاص الذين يشترون سِلعاً كملابس متناسبة خصّيصاً مع قياس الأشخاص، ويرسلون لهم معلومات عن خطط لفقدان الوزن.

بالنسبة إليّ، كان كل ذلك بداية عصرٍ مناورة مالية. هناك شركات كبرى تسعى لاستخدام بيانات شخصية كي تفرض سلطتها عليّ. لذلك، شعرتُ بأن كِذبتي مبرَّرة لجهة إعادة التوازن إلى العلاقة.

لكن السؤال الأخير لبوك استوقفني. ما سيكون عليه حال العيش في عالم حيث يكون للكل هويات زائفة؟

لقد حاولت تخيُّل ذلك العالم. هو عالم حيث لا يمكنكم الثقة بأشخاص لا تعرفونهم في الواقع، ولا تلجون بريداً إلكترونياً لشخص يدّعي بأنه صديق صدوق، وحيث لا يمكنكم الثقة بمراجعات مصدر غير موثوق. ربما يكون نوعَ العالم حيث يمكن خداع نجم كرة قديم شهير للوقوع في غرام امرأة التقاها عبر الإنترنت؛ والمرأة في الواقع شخصية خيالية ابتكرها رجل أُغرِم به. (لأولئك الذين لا يعرفون، لقد وصفتُ قصة مانتي تيو، الظهير في فريق نوتر دام). قد لا أملك مخيّلة كافية، ولكن الأمر يبدو شبيهاً جداً بالعالم الذي نعيش فيه اليوم.

وماذا عن الاحتكام إلى أشخاص منطقيين؟ فالأشخاص الذين استشرتهم ظنّوا أنني غبية لمجرّد السؤال عن المبادئ الأخلاقية لكِذبة غير مؤذية. برأي زوجي، لا بأس باعتماد أسماء زائفة ما دمت لا أحصل على بطاقة هوية زائفة. وبرأي عرّابة صغيرَيّ، لا يحتاج الأمر لأي تفكير؛ لقد سبق لها أن اعتمدت عدة عناوين بريد إلكتروني مختلفة زائفة استخدمتها في مظاهر مختلفة من حياتها. وبرأي إحدى زميلاتي، إنها فكرة رائعة، وشرعت في الحال بإعداد حسابات بأسماء زائفة.

كانت عيّنة صغيرة، ولكنني قررت إخضاع كَذِبـي لاختبار الإعلان جَهاراً.

á á á

مع التزامي الجديد بالكَذِب، استجمعتُ قواي وبدأتُ ثانيةً بهوية آيدا على الإنترنت. هذه المرة، كنت جدّية: سأحصل على بطاقة ائتمان لآيدا تاربيل.

حصلتُ على فكرة بطاقة ائتمانٍ لآيدا من مفكك الشيفرة جون كالاس. كان قد قدم إلى مكتبـي ليُريني تطبيقات وضعها تسمح لكم بفك شيفرة اتصالات ونصوص من جهاز آي فون. فأطلعته على كفاحي لبناء هويّة

دَورية قوية. بسهولة كبيرة، أخرج محفظة جَيبه وبسط على شكل مروحة صفَّ بطاقات هوية بأسماء مختلفة - بما فيها تلك التي تحمل اسم دايل بـي. كوبر، تيمّناً بالعميل الخاص في الأف بـي آي الذي ظهر في البرنامج التلفزيوني في التسعينات تْوين بيكس .

الأمر سهل، قال لي. أَخبري شركة بطاقات الائتمان بأنك تريدين بطاقة جديدة باسم جديد يُضاف إلى حسابك. يقوم الأهل بذلك في كل الأوقات لأجل صغارهم.

آها. لقد فهمتُ. إنها مسألة رفع مستوى الأمن الكمبيوتري إلى الدرجة الفُضلى. لم يكن إخفاء هويّتي عن شركة بطاقة الائتمان التهديدَ، بل إخفاء هويّتي حيث أُنفق المال. فلو كنت مشتبَهاً بها بارتكاب جريمة، يمكن لمدّعٍ عام إرسال استدعاءٍ لـأمريكان إكسبريس للمثول أمام المحكمة كي يعرف الهويّة الحقيقية لآيدا تاربيل.

فقرّرت القيام بذلك. لقد حاولت طلب بطاقة جديدة عبر موقع أمريكان إكيبريس على الويب، ولكن الموقع قال إنه يتعيّن عليّ الاتصال. أخيراً، اتصلت من المكتب ذات مرة في وقت متأخر من الليل عندما لم يكن أحد في الجوار. كنت ما أزال أشعر بالخجل. لم أشأ أن يقوم أي فرد من عائلتي - أو في المكتب- باستراق السمع عليّ.

بالطبع، لم يتكدّر ممثل خدمة الزبائن البتّة بسبب طلبـي ربط بطاقةٍ إضافية بحسابـي. فسأل عن تاريخ ولادة آيدا - لحسن الحظ، كنت أملك هذه المعلومة لأنني أعددت حساب البريد الإلكتروني باسمها. وعندما سأل عن رقم ضمان آيدا الاجتماعي، قلت إنني لا أعرفه. لم يرفّ له جفن، بل واصل عمله. ستكون البطاقة في البريد في غضون أيام قليلة، قال.

مرّت أيام قليلة، ولم أستلم أية بطاقة. ومرّ أسبوع، ومن ثم أسبوعان. أخيراً، اتصلت وطلبت بطاقة أخرى. مرّ أسبوع ولم تصل تلك البطاقة أيضاً.

في غضون ذلك، شرعت بتلقّي رسائل بريد إلكتروني واتصالات من أمريكان إكسبريس تسألني عن رقم ضمان آيدا الاجتماعي. كانت الاتصالات المؤتمَتة تقول، "إضغطي على الرقم 1 إذا كنت آيدا، واضغطي على الرقم 2 إذا لم تكوني آيدا. إضغطي على الرقم 1 إذا كانت آيدا متوافرة، وعلى الرقم 2 إذا لم تكن متوافرة". فشعرت بأنني في مأزق: لم أكن آيدا ولم أُرِد البَوح بأنني لست آيدا أريد . لذلك، أنهيت المكالمة الهاتفية.

وبدأت باالتفكير في ما إذا كان رقم الضمان الاجتماعي الناقص يؤخّر البطاقة. ولكنني أرغمت نفسي على الاتصال مرة أخرى. قالت الممثلة إنها

ستُرسل لي بطاقة جديدة على وجه السرعة.

ووصلتْ في اليوم التالي - جميلة، برّاقة، خضراء، واسم آيدا بحروف نافرة. لم يسبق لي أن أحببت بطاقة بهذا القَدْر. في ذلك المساء، عندما عاد زوجي من العمل إلى المنـزل، أرَيتُه البطاقة بفخر.

"أوه!" قال. "لماذا لم تُخبريني بأنك آيدا تاربيل؟ كنت أتخلّص من بريدها الإلكتروني طوال أسابيع".

ملاحظة لي: في المستقبل، حذِّري زوجك قبل إعداد هويّة زائفة.

á á á

الآن، آيدا بحاجة إلى عنوان بريديّ جديد.

بعد رؤية ملفاتي المتوافرة لدى وسطاء البيانات، اتّضح لي أنه إذا بدأت آيدا بتلقّي بريد على عنواني بشكل منتظم، ستبدو في سجلاتي، في نهاية المطاف، كشريك أو فرد من العائلة.

وفكّرتُ مليّاً في تأمين صندوق بريد لآيدا، ولكن مكتب البريد يطلب من المستخدمين تقديم بطاقة تعريف لدى حصولهم على طُرود. لم ينجح الأمر. فتحققت من يو بيي أس ستور ولكنه يعتمد السياسة نفسها.

لذلك، أقنعتُ صديقةً بالموافقة على تلقّي بريد آيدا وطُرودها. تعيش صديقتي في مبنى سكنيّ كبير حيث يُفرز بريد كل مشترك داخل صناديق بريد مماثلة في الحجم لصناديق مركز البريد. وكل ما تعيّن عليّ القيام به هو إلصاق اسم آيدا تاربيل داخل صندوق البريد. وبسرعة، بات لآيدا عنوان.

بوجود بطاقة ائتمان وعنوان، أصبحت إمكانات آيدا لا محدودة. مع ذلك، أردت الاحتراس في شأن حساباتها عبر الإنترنت.

فاستشرتُ مايكل ساسمان، المدّعي العام السابق في وزارة العدل الذي يعمل الآن كمحامٍ خارجي لصالح شركات مثل غوغل. فقال لي إن معظم الخدمات على الويب تحتفظ بتسجيل عنوان الإنترنت إلى الأبد، لذلك يجدر الحِرص على المكان الذي أُعِدُّ حساباتي منه.

وهكذا، أطلقتُ حياة آيدا عبر الإنترنت من خلال اصطحاب جهازي الحضني إلى مقهى يحتوي على خدمة واي - فاي مجّانية. فجلستُ، وطلبت كابوتشينو، وفتحت جهازي الحضني، وشغّلتُ تور (Tor)، برنامج إخفاء الهوية الذي يُخفي عنوان الإنترنت لجهازكم من خلال إرسال حركة الاتصالات إلى مختلف أنحاء العالم. هذه المرة، بدوتُ أنني في ألمانيا.

وتصفُّح تور بطيء. لاختبار هذا الأمر، أدخلتُ عنوان جامعة نيويورك

على الويب، www.nyn.edu ، إلى متصفّح تور ومتصفّح فايرفوكس ويب (Web Firefox)، وشغّلتُ توقيت كل منهما. لقد تطلّب الأمر عشرين دقيقة في تور، وثلاث ثوانٍ في فايرفوكس. كان لديّ على الأقل كثير من الوقت لارتشاف قهوتي أثناء التصفّح عبر تور.

وشرعت بالاشتراك في حساب مجّاني للبريد الإلكتروني باسم آيدا عبر Outlook.com من مايكروسوفت. فقوّيتُ قلبي وأدخلت رقم 212-867-5309 على أنه رقم هاتفها (اخترته تيمّناً بأغنية تومي تيتون الشهيرة التي تعود للثمانينات). وأطفأتُ ميزة الإعلانات المستهدفة.

شاعرةً بسرور ذاتيّ تام، أعددت أيضاً حساباً لآيدا على أوبن تايبل (OpenTable)، مستخدمةً عنوان آوتلوك. لقد تركتُ خانة إدخال رقم الهاتف فارغة. (لا أعرف سبب عدم تبادر هذه الفكرة إلى ذِهني من قَبل). بعد ذلك، أعددت حساباً لآيدا على Amazon.com ، مستخدمةً عنوان صديقتي البريدي ورقم بطاقة ائتمانها. ورفضتُ طلب أمازون تزويدَ آيدا بـ"توصيات أمازون" التي يُضفى عليها طابع شخصي.

فأول كتاب طلبتُه هو نسخة مستعمَلة لرقابة رِزم بيانات: برنامج معرفة المكتبات. نُشر الكتاب عام 1991، وهو سرد لجهود الأف بـي آي في الثمانينات لتجنيد أُمناء المكتبات كي يتجسسوا على الكتب التي يتفحّصها الأجانب، وهو البرنامج الذي حثّ كل ولاية تقريباً على تبنّي قوانين لحماية سرّيّة سجلات تَداولِ الكتب في المكتبات.

كانت دُعابتي حيال الخصوصية: استخدام اسم زائف لطلب كتاب يتناول سبب حماية خصوصية الكتب.

á á á

تطلّبني الأمر بعض الوقت لأعرف متى يتعيّن عليّ أن أكون آيدا ومتى يتعيّن عليّ أن أكون ذاتي.

لقد طلبت آيدا كل كتبـي من أمازون، وأجرت كل حجوزاتي في المطاعم، ودفعت ثمن وجباتي في المطاعم عندما كنت ألتقي شخصاً لإجراء مقابلة معه. سرعان ما بات لديّ عشرات الحسابات على الإنترنت باسم آيدا، ووضعتُ برنامج جدول بيانات يحتوي على كل تسجيلات دخولاتها وكلمات مرورها.

ولكنني علمتُ بوجود بعض الأمور التي لا يمكن لآيدا القيام بها. لقد حاولتُ استخدام بطاقة ائتمان آيدا في متجر السِّلع الرياضية موديل، فطلب الموظف الكتابـي معلومات شخصية لمقارنة بطاقة ائتماني. لذلك، دفعتُ

نَقداً. حدث الأمر نفسه في أولد نايفي ولكن ليس في متجر الملابس الكلاسيكية الأنيقة حيث اشترت آيدا كنـزة صوفية دون مواجهة أية مشكلة. كان يتعيّن على آيدا المواظبة على متاجر الملابس الأنيقة.

لقد جعلتني آيدا أُدرك الأماكن التي أُعرف فيها باسمَين. فعندما جلست في حانتي المفضَّلة قرب مكتبـي، رحّبت بـي الساقية باسمي، قائلةً، "مرحباً، يا جوليا". لقد تفاجأتُ بمعرفتها لاسمي - بالرغم من قيامنا بتبادل أطراف الحديث في الحانة في غالب الأحيان، لم أذكر إطلاعي إيّاها على اسمي. لقد أدركتُ أنها لا بد من أن تكون قد عرفتني من بطاقة اعتمادي. وأدركتُ أيضاً أنني قد أُثير الشُّبهة إذا غيّرت هويّتي فجأةً. لذلك، عندما حان وقت الدفع للساقية، أعدت بطاقة آيدا تاربيل إلى حقيبة يدي وأخرجتُ بطاقة جوليا أنغوين.

وكلّما استخدمتُ آيدا ازداد قلقي حيال الإفراط في استخدام هويّتها. سيصبح لديها في وقت قريب رقم قياسيّ في الائتمان. كانت آيدا قد بدأت بتلقّي عروض للحصول على بطاقات ائتمان من شركات أخرى. (تقول أمريكان إكسبريس إنها لا تبيع أسماء زبائنها، لذلك تبقى كيفية دخول آيدا قوائم التسويق أمراً غير واضح). لو لم أتوخَّ الحذر، لانتهى الأمر بآيدا في تقارير الأسماء المستعارة التي يُعدّها وسطاء البيانات.

لقد أدركتُ أنني أريد مزيداً من الهويات الزائفة للتخفيف من العبء المُلقى على عاتق آيدا.

á á á

لم أكن أملك الطاقة الفكرية لبناء آيدا أخرى، وهو أمر يستدعي ابتكار تاريخ مَولد لها ومسقط رأس وكلمات مرور، واستجماع الشجاعة لابتكار أكاذيب في شأنها.

أردت طريقة أكثر سهولة وسرعة لابتكار هويات زائفة.

لقد وجدت أن هناك كمّاً كبيراً من الخدمات التي تسمح لكم بابتكار عناوين بريد إلكتروني يمكن التخلص منها - في الغالب لتجنّب إغراق الإنترنت بعدة نسخات من الرسالة نفسها (message Spam). على سبيل المثال، إذا ابتكرتُ حساباً على موقع ويب يدعى spamgourmet.com ، يمكنني ابتكار عناوين بريد إلكتروني فريدة لتسجيل دخولي إلى كل موقعٍ على الويب.

ولكنني كنت كسولة مرة ثانية: لم أشأ ابتكار هويات بريد إلكتروني جديدة. لذلك، بدأت باستخدام خدمة مجّانية تُدعى ماسك مي (MaskMe

)، من شركة في المرحلة الأولى من عملياتها تدعى إيْبِن، تبتكر عنوان بريد إلكتروني زائف جديد لكل حساب. على سبيل المثال، عندما تطلب مني ForeignPolicy.com ابتكار حساب لقراءة مقالة، تبتكر ماسك مي عنوان بريد إلكتروني كي أستخدمه لتسجيل دخولي: a@opayp.com 18123 . وترسل ماسك مي لي كل رسائل البريد الإلكتروني الموجَّهة من ذلك العنوان. ولكن إذا قام موقع ويب بإرسال عدد كبير من رسائل البريد الإلكتروني، باستطاعتي إبلاغ ماسك مي كي تحجبها.

لقد استمتعتُ بحجب رسائل البريد الإلكتروني. فبعد تلقّي ثلاث رسائل من كلاوت، وهي شركة رئيسية ذات تأثير اجتماعي سجّلتُ دخولي إليها أثناء تدقيقي، قمت بحجبها. وبعد تلقّي سبع رسائل من RecordedFuture.com ، وهي شركة كبيرة لتحليل البيانات، قمت بحجبها.

واشتركتُ أيضاً في خدمة فذّة من ماسك مي لقاء 5 دولارات في الشهر أصدرتْ لي رقم هاتف جديد يمكنني إرساله إلى أي هاتف. الآن، بات بإمكاني إدخال رقم هاتفي إلى الاستمارات دون القلق من تلقّي اتصالات تسويقية مزعجة.

لقد بدأتُ بإدراك طريقة عمل هذا الكَذب الصعب. إن أفضل طريقة للقيام به هو أتمَتته.

á á á

ولكن من الصعب أتمَتة الخداع في آلة تسجيل النقد.

بالطبع، يمكنني استخدام السيولة النقدية على الدوام، وهي في الغالب مجهولة المصدر بالرغم من عدم تحبيذها لأنها ليست على الموضة. فالأوراق النقدية الأميركية تحتوي على أعداد متسلسلة، ويلجأ بعض المصابين بذُهان الارتياب في شأن الخصوصية إلى استبدال السيولة النقدية لتجنّب تعرّضهم للتعقُّب من خلال الرقم المتسلسل. ولكن بالنسبة إلى رفع مستوى أمني الكمبيوتري إلى الدرجة الفُضلى - تجنُّب شبكات التعقُّب - فالسيولة النقدية جيدة.

ولكن حمل مقدار كبير من السيولة النقدية هو أمر غير عملي وغير حكيم في غالب الأحيان. لقد حاولتُ فَطم نفسي عن بطاقات الائتمان، ولكنني واصلت تفضيلها - لأنني أحب في الغالب تتبّع أثر إنفاقي، وأكره حشوَ محفظة جَيبي بإيصالات سيولة نقدية ومحاولةَ تذكّر تدوينها في وقت لاحق.

وحاولت استخدام بطاقة ائتمان مُسبَقة الدفع تحتوي على 200 دولار

اشتريتها من صيدلية لقاء سيولة نقدية. لقد استخدمتها لأجل عمليات شراء صغيرة - غداء قرب مكتبـي، قهوة، سِروالان قصيران بقيمة 27 دولاراً من جي كرو. لقد أحببت ما كُتب على الإيصالات " MyGiftCard " حيث يكون الاسم في العادة، ولا يرفّ جَفن لأمناء الصندوق عندما أسلّمهم إيّاها. ولكن مع انخفاض رصيد البطاقة، كففتُ عن استخدامها. لقد شعرت بأنه من السخف الطلب من موظف كتابـي تعبئة البطاقة بمبلغ 5,32 دولاراً وقيامي بدفع البقية نَقداً. وأكره أيضاً إنفاق الدولارات المتبقية.

لذلك، اختبرتُ وسيلة أخرى: رقم بطاقة ائتمان في المتناول. إنها أرقام سابقة يمكن استخدامها لدى تاجر واحد. في الواقع، هي بطاقات اعتماد مُسبَقة الدفع يتم إصدارها لكل عملية تجارية. لقد حصلتُ على أرقام بطاقة اعتمادي التي يمكن التخلص منها من ماسك مي بريميوم (MaskMe Premium)، وهي الخدمة نفسها التي زوّدتني بعناوين بريد إلكتروني وأرقام هاتف في المتناول.

كانت محاولتي الأولى لاستخدام رقم بطاقة اعتمادي كارثية. أردت استبدال قمصان اليوغا البالية بأخرى جديدة. لذلك عثرت على القمصان على الإنترنت ووضعتها في سلّة تسوّقي عبر الإنترنت. وأدخلتُ من ثم اسمي وعنواني الحقيقيَّين لأجل الشحن والفواتير. عندما احتسب موقع الويب الثمن - بما في ذلك الشحن - أنتجت ماسك مي رقم بطاقة اعتماد يمكنني استخدامه لأجل قيمة العملية التجارية بالتحديد. ولكن البطاقة رُفضت. وحاولتُ مجدداً، ولكنني حصلت على الرسالة نفسها: دفع قيمة العملية التجارية مرفوض.

ووجدت نفسي في مأزق. يبدو أن ماسك مي تعتقد أنه سبق لي أن دفعتُ المبلغ. لقد ذكر رقمُ بطاقة اعتمادي أن المال أُنفق. ولكن موقع الويب لم يظنّ أنه دُفع. لقد ضاع مالي في مكان ما في الأثير.

بعد ساعة قضيتها على الهاتف مع إيْبِن، فهمتُ خطأي: أنا بحاجة إلى إدخال عنوان إيْبِن ليكون عنوان فواتيري. في غضون ذلك، اتصلتُ بموقع الويب، وألغيت العملية التجارية، وطلبتُ القمصان عبر الهاتف بواسطة رقم بطاقة ائتماني العادي.

بعد أسبوع، حاولتُ ثانيةً، واشتريت أسطوانة مُدمَجة تحتوي على أغان شعبية للصغار من سميثسونيان - مستخدمةً عنوان إيْبِن عنواناً لفواتيري. هذه المرة، تمكنتُ من الولوج بدون أية مشكلة. بئس الأمر. بالطبع، بدا الأمر برمّته سخيفاً قليلاً لأنني كنت ما أزال أوفّر اسمي وعنواني الحقيقيَّين

كي يتم شحن سِلَعي. فقررت محاولة العثور على عملة مجهولة المصدر أكثر فأكثر.

لقد أَمِلتُ في شراء نقود رقمية، عملة رقمية فعلية كانت صرعة الموسم في مجتمع المتسلّلين إلى ملفات الكمبيوتر. ولكنني لم أتمكن من إيجاد مكان يسمح لي بشراء نقود رقمية بواسطة بطاقة اعتماد. لقد أرادوا كلهم رقم حسابي المصرفي أو عملية تحويل بواسطة التلغراف - لأن الناس يتصلون في غالب الأحيان، كما يبدو، بشركة بطاقة الائتمان الخاصة بهم ليشكوا من عدم تلقّيهم نقودهم الرقمية.

يمكن استخدام النقود الرقمية في الأسواق السوداء عبر الإنترنت التي يمكنها بيع عقاقير وأسلحة. مع ذلك، بدأت بعض مؤسسات الآجرّ والملاط بقبول نقود رقمية. ففي أيار/مايو 2013، قضى كَشمير هيل، وهو مراسل لـ فوربس ، أسبوعاً على النقود الرقمية دون سواها - حاصلاً على غذائه من خلال خدمةٍ لتسليم الطعام في سان فرانسيسكو يَقبل العملة.

مع ذلك، تكون كل العمليات التجارية بواسطة النقود الرقمية مسجَّلة ويمكن رؤيتها علَناً. ولا تُرفَق أسماء الأشخاص بعملياتهم التجارية، ولكن باستطاعة محقِّق عازم أن يحدد، على الأرجح، هوية الأشخاص الذين يقفون وراء بعض العمليات التجارية بواسطة النقود الرقمية. لم أكن أسعى وراء إخفاء المصدر.

á á á

كلما تعمّقتُ في العمليات التجارية الرقمية المجهولة المصدر، قلّت محبتي لها أكثر فأكثر. كانت تبدو ملاذات للمجرمين.

في العام 2007، اتُّهمت شركة في المرحلة الأولى من عملياتها، وتدعى إي - غولد، بتبييض أموال. قالت لائحة التُّهَم إن الشركة كانت تعرف أن خدماتها مستخدَمة من قِبَل سارقي هويات (منتحلي شخصيات)، منتجي أفلام إباحية للصغار، ومجرمين آخرين. في العام التالي، اعترفت الشركة ومالكوها بالذَّنْب في مسألة تبييض الأموال. وفي العام 2013، أغلق المدّعون العامون الفيدراليون موقع ليبرتي ريزرف (Reserve Liberty) لصرف العملات عبر الإنترنت، موجِّهين له تُهمة تبييض أموال بقيمة 6 بلايين دولار لمنتجي أفلام إباحية للصغار ومجرمين آخرين. "لو كان آل كابون حيّاً اليوم، لَخبّأ ماله بهذه الطريقة"، قال ريتشارد ويبر، رئيس قسم التحقيق الجنائي في دائرة الإيرادات الداخلية.

حتى إن بعضهم تنبأ بإمكانية تسبُّب تلك العمليات التجارية المالية

المجهولة المصدر حقاً بتفكك المجتمع. ففي العام 1996، نشر جيم بِل، الذي أعلن نفسه فوضويّاً، مقالةً على منتدى عبر الإنترنت بعنوان "سياسات الاغتيال"، واصفاً كيف يمكن للنقود المجهولة المصدر تسهيل وضع جوائز نقدية للناس الذين "يتنبّأون" بشكل صحيح بوفاة أحدهم. "قد يكون بالإمكان وضع جوائز مماثلة دون أن يعرف أحد مَن ربح المال، بل يعرفون فقط أن الجائزة مُنحت". وصف بِل سوق التنبُّؤ بالوفاة بأنها طريقة لمعاقبة "منتهكي الحقوق" من خلال وضع سعر على رؤوسهم. "تأمّلوا بمدى إمكانية تغيُّر التاريخ لو كنا قادرين على قتل لينين، ستالين، هيتلر، موسوليني، توجو، كيم إيل سونغ، هو تشي مْنِه، آية الله الخُميني، صدّام حسين، معمر القذافي، وسواهم، إضافةً إلى كل البُدلاء عند الضرورة، لقاء بضعة ملايين قليلة من الدولارات"، كتب.

لم يتم تلقّي فكرة بِل بوضع "مكافآت" على رؤوس موظفين حكوميين بشكل جيد. ففي العام 1997، أغار عملاء دائرة الإيرادات الداخلية على منـزل بِل. لقد اتُّهم بإعاقة العدالة واستخدام أرقام ضمان اجتماعي زائفة، وحُكم عليه بالسجن لمدة أحد عشر شهر.

من الواضح أن بِل كان يراقب موقفاً متطرفاً. ولكن مقالته حملتني على التفكير مليّاً في سؤال سيسيلا بوك الأخلاقي: ماذا يحدث لو كذب كل من في وضعكم؟

وبدأت بالتفكير في أن ما أريده حقاً ليس الغُفلية بل الحصانة. أردت التحصن من عواقب معاملاتي التجارية غير المنطقية. لم أشأ تعريض الأشخاص الذين يتناولون الغداء معي لشُبهة تمرير معلوماتٍ لصحافية. لم أشأ لمشترياتي أن تَسِمني بـ"المُنفِقة الكبيرة" كي لا تُعرض عليّ حسومات عبر الإنترنت. لم أشأ أن يُشتبه بـي بأنني فوضوية بعد التحرّي عن النقود الرقمية. ولكنني لم أتوقع أو أشأ حصانةَ معاملاتٍ تجارية جنائية.

لقد ذكّرتني رغبتي في أن أكون حصينة من عواقب التجارة بالتأمّل الجميل لعالِم الأنتروبولوجيا، ديفيد غراوبر، حول معنى الدَّين ومعانيه الأخلاقية الضمنية. ففي كتابه الدَّين: أول *5,000* عام ، يصف غراوبر وجود ديون لا يُفترض تسديدها أبداً، كدَيننا لأهلنا أو دَينٍ للُطفٍ طَوعيّ.

بعض الديون فقط يمكن تسويتها بالمال. فلتلك الديون بعض المميِّزات، يقول. إنها ديون بين "متساوين محتمَلين" ولكنهم "ليسوا حالياً في حالة المساواة" يستخدمون المال لإصلاح الأمور. "الدَّين... هو مجرد تبادل لم يُنجَز"، يكتب.

أدركتُ أن الحصانة التي أريد مماثلةٌ لما يسعى إليه المَدين: أردت تسديد ديوني بالكامل - فأعود إلى حالة مساواة مع مَديني - بعد إتمام معاملتي الجارية.

ولكن في اقتصاد البيانات الشخصية، يبدو أنني لن أتحرر من ديوني أبداً. فكل معاملاتي التجارية ستلازمني إلى الأبد، ملاحقةً إيّاي ومُبلِغةً إيّاي الخيارات المتوافرة لي. وهكذا، سيكون عليّ الاتكال على آيدا وهويّاتي المخفيّة لتسديد ديوني، حتى أتمكن من إيجاد طريقة أفضل.

الفصل العاشر
قُمامة الجَيب

وقفتُ تحت برج الساعة العالمي في ألكسندربلاتز في برلين، شاعرةً بالتوتر. كنت قد وصلت للتوّ إلى المدينة وتدبّرت لقاء جاكوب أبلبوم، وهو الباحث في أمن الكمبيوتر الذي تم التحقيق ببريده الإلكتروني سرّاً من قِبَل الحكومة الأميركية بعد كشف النقاب، عام 2010، عن تطوّعه للعمل لصالح ويكيليكس. ولكنني لم أجد سبيلاً للاتصال به - لا رقم هاتف محمول، لا عنوان شارع، لا شيء. تعيّن عليّ الانتظار ببساطة للتحقق مما إذا كان سيحضر إلى مكان اللقاء المتفَق عليه.

لقد قطعتُ نصف المسافة حول الكرة الأرضية لأجل هذا اللقاء، ولكنني لم أضع خطة احتياطية بديلة إذا لم يحضر. شعرت بأنني مكشوفة.

هذا ما يتطلبه الأمر للقيام بعملي كصحافية في عالم حيث يمكن تعقُّب مكان وجودي عن بُعد من خلال هاتفي المحمول. يعني ذلك أنه يجب عليّ التقاء بعض مصادري الحساسة شخصياً بدون مساعدة تكنولوجيا رقمية.

وهكذا، وقفت بحَرَج تحت الساعة التي كانت طوال عقود من الزمن نقطة لقاء الناس في برلين. فكل من يحيط بي يتحقق من هاتفه. لقد تخيّلتهم يوجهون رسائل نصّيّة لأصدقائهم بتلك العبارات المطمئِنة - "أين أنت؟" "في طريقي إليك" - التي تُمثّل الامتياز الحصريّ للعصر الرقمي. لم أكن أملك طمأنة رقمية مماثلة.

وألقيت نظرة سريعة على رجل طويل الشعر يُقفل على دراجته. هل هو جايك؟ لقد خطر ببالي أن أكون قد رأيت صورته على الإنترنت فقط - ربما يُخفي هويّته من خلال استخدام صورة قديمة العهد أو غير دقيقة. ولكن راكب الدراجة أخرج هاتفاً محمولاً لإجراء اتصال، لذلك اعتبرتُ أنه ليس جايك. بعد دقائق قليلة، استقرّ نظري على رجل يضع نظارة ذات حرف معدني ولا يحدّق بهاتف. ربما يكون جايك؟ ولكنه لم ينظر إليّ، وبعد دقائق قليلة لوّح لرجل في الناحية المقابلة للميدان.

أخيراً، وبدون أي إنذار، ظهر جايك إلى جانبي تماماً. كان يبدو كما توقعتُ تماماً. وبما أنه يمكن العثور على صورتي بسهولة عبر الإنترنت، فقد عرفني على الفور. تنهّدتُ ارتياحاً أثناء توجهنا إلى مقهى قريب للتحدث.

في النهاية، اعترفت بأن هاتفي المحمول موجود في حقيبة يدي. كنت أعرف أنه لم يكن يُفترض بـي اصطحابه معي، ولكنني رميته في حقيبتي في اللحظة الأخيرة. كنت في مدينة غريبة وخشيتُ من اضطراري لاستخدامه بطريقة ما.

"لقد أطفأتُه"، قلت بطريقة اعتذارية.

"ها!" ضحك جايك وسأل "كيف تعرفين أنه مُطفأ؟ هل أزلتِ البطارية؟ ربما زُرع برنامج تجسسي لجمع المعلومات في هاتفك لإرغامه على مواصلة نقل معلومات حتى ولو بدا أنه مطفأ".

في وقت من الأوقات، اعتقدت أن جايك مصاب بذُهان الارتياب قليلاً. فكونه متطوّعاً في ويكيليكس ويُعتقل في غالب الأحيان عند الحدود الأميركية، يتكيّف جايك إلى حد بعيد مع تهديدات الرَّقابة أكثر من معظم الناس. ولكنه مُحِق في هذه الحالة. فبعد نحو عام من لقائنا، ألقى إيرا "غاس" هانت، الرئيس التنفيذي للتكنولوجيا في السي آي أيه، خُطبة تتفاخر بقدرة الوكالة على اقتفاء أثر أجهزة متحركة. "أنتم تَعون واقع قدرة شخص ما على معرفة مكان وجودكم في كل الأوقات، لأنكم تحملون جهازاً محمولاً، حتى ولو كان ذلك الجهاز المحمول مطفأ"، قال هانت في خُطبة بعنوان "التحديات الكبرى للسي آي أيه مع البيانات الضخمة". "تعرفون هذا الأمر، كما آمل؟ أجل؟ حسناً، يُفترض بكم ذلك".

ما يزال من غير الواضح بالتحديد إلى أية تكنولوجيا تعقُّب يشير هانت. ولكن الأف بـي آي طلبت، في العام 2006، وحصلت على أمر صادر من المحكمة لتثبيت "فيروس متنقل" على هاتف رجل عصابات مكّن العملاء من التنصت حتى عندما يكون هاتفه مطفأ. كان جايك يؤكد ما يعرفه وآخرون: هواتفنا المحمولة هي أجهزة التعقُّب الأكثر فعالية في العالم، حتى عندما تكون مطفأة.

á á á

في تقنيات التجسس، هناك العبارة الحديثة "قُمامة الجَيب". هي تعني، حرفياً، قُصاصات الورق وأشياء أخرى يمكن العثور عليها في جَيب شخص ما. وغالباً ما تحتوي هذه الأشياء على معلومات عن صِلات الشخص - أرقام هاتف، عناوين، رقم حساب - يمكنها المساعدة في تحقيقٍ يُجرى عنه.

اليوم، تحتوي جيوبنا على القُمامة الأساسية: هواتف محمولة هي كناية عن أجهزة كمبيوتر مصغَّرة يمكن العثور فيها على دفتر عناوينا بأكملها، وكل اتصالاتنا المكتوبة تقريباً، وصورنا، وموسيقانا، لا بل أيضاً الألعاب التي

يمكننا ممارستها.

والأسوأ من ذلك أنه يمكن رؤية قُمامة جيوبنا الإلكترونية عن بُعد. فوفقاً للأساليب القديمة، كان يتعيّن على عملاء إنفاذ القانون اعتقال مشتبَه به قبل التمكن من البحث في جيوبه. الآن، باستطاعة مشغِّلي شبكات التعقُّب التجارية والحكومية رؤية موقعِ وبعض محتويات هواتفنا عن بُعد - من خلال طلب معلومات من موفِّري خدمات الاتصال عبر الهواتف المحمولة.

إن المثال الأكثر فظاعة عن مراقبة الهواتف المحمولة هو، بالطبع، البرنامج الذي كشف عنه المتعاقد السابق مع وكالة الأمن القومي، إدوارد سنودن، الذي تلقى طوال سبع سنوات كلَّ سجلّ تملكه شركات الهاتف عن الاتصالات التي أُجريت في الولايات المتحدة. ووصف الرئيس أوباما البرنامج بأنه يجمع "الاتصالات الثنائية". لقد أعطى وصفاً أميناً للغاية: "رقم هاتفكم يتصل برقم هاتفي. لا أسماء، لا محتويات في قاعدة البيانات تلك. كل ما يوجد في البرنامج هو الاتصالات الثنائية، متى جرت تلك الاتصالات، وكم دامت".

تتعقّب غالبية أقسام الشرطة المحلية أيضاً استخدام الهاتف المحمول من خلال التقدم بطلبات سرّية إلى شركات الهواتف المحمولة، ودون الحصول على مذكرات تفتيش في غالب الأحيان. ففي العام 2011، استجاب أبرز الموفِّرين الأميركيين لخدمات الاتصال عبر الهواتف المحمولة لـ1,3 مليون طلبِ إنفاذٍ للقانون بالحصول على معلومات عن مشتركين، بما فيها موقع المتصل. على سبيل المثال، قالت أيه تي إند تي إنها استجابت لنحو سبعمئة طلب في اليوم - نحو ثلاثة أضعاف عدد الطلبات التي تلقّتها عام 2007.

ومع ازدياد عمليات تعقُّب الهواتف المحمولة بدون مذكرات، شرع بعض القضاة بالتساؤل عن قانونيّتها. فمنذ العام 2005، كتب أكثر من عشرة قضاة مساعدين لقضاة المحاكم الجزئية تعليقاتٍ يُنكرون فيها تلقّي طلبات للحصول على أمر من المحكمة لتعقُّب هواتف محمولة. بدأ العصيان عام 2005 عندما رفض ستيفن سميث، وهو قاضٍ مساعد في المحكمة الجزئية الجنوبية في تكساس، طلباً حكومياً بالحصول على البيانات الفورية لمواقع الهواتف المحمولة. تحدّى سميث النظرية القانونية "الإبداعية" التي تبرّر عدم الحاجة إلى مذكرة تفتيش. بعد قرار سميث، شرع القضاة المساعدون في مختلف أنحاء البلد برفض طلباتٍ للحصول على بيانات مواقع الهواتف المحمولة دون إصدار مذكرات.

وانقسمت محاكم أعلى حول ولوج السجلات التاريخية لبياناتِ مواقع الهواتف المحمولة. ففي العام 2010، حكمت محكمة الاستئناف للدائرة الثالثة بامتلاك المساعدين القضائيين حرّية وجوب استصدار مذكرة تفتيش بهدف الحصول على السجلات التاريخية للهواتف المحمولة، بالرغم من "شعورنا بالإحباط بسبب إخفاق الكونغرس في إيضاح نيّته". ولكن محكمة الاستئناف للدائرة الخامسة انقلبت في العام 2013 على قرار القاضي سميث المتخَذ عام 2010 لتمنع الحصول على السجلات التاريخية لمواقع الهواتف المحمولة بدون مذكرة. "نفهم رغبة مستخدمي الهواتف المحمولة في المحافظة على خصوصية المعلومات المتعلقة بمواقع هواتفهم..."، كتبت القاضية إديث براون كليمنت. "ولكن تحقيق هذه الرغبات موجود في السوق أو في العملية السياسية".

إلى أن تعالج المحكمة العليا أو الكونغرس المسألة، تبقى شبكات تعقُّب الهواتف المحمولة قانونَ الأرض.

á á á

ما مدى أهمية قُمامة الجَيب؟ إن الشخص الذي نتصل به، وتاريخ اتصالنا به، يمكن أن يكون مُلهِماً بقدْر ما نتحدث بشأنه عبر الهاتف.

طالما اعتمد الجواسيس الذين لا يُجيدون قراءة محتويات رسائل أعدائهم على ما يُعرَف بـ"تحليل حركة الاتصالات" - دارسين أنماط المرسِل، والمتلقّي، والوقت، وطول الرسائل. ففي الحرب العالمية الأولى، واجه الفرنسيون صعوبة في فك الشيفرة الألمانية - المعروفة بشيفرة ADFGVX . ولكنهم كانوا يعرفون أن الشيفرة استُخدمت لنقل أوامر وتوجيهات لأجل التقدّم على جبهة ما، لذلك تمكنوا من التنبّؤ بالوقت التقريبـي للهجمات الألمانية أثناء ربيع وصيف العام 1918. وحتى عندما غيّر الألمان إشارات الاتصالات اللاسلكية - الأحرف التي تحدد هوية المرسِل - تمكّن محللو حركة الاتصالات الفرنسيون من تمييز الاتصالات عبر أنماط أخرى. "قبل عدة أيام من القيام بعملية عسكرية، كان حجم الرسائل التي يتم اعتراضها يزيد على الدوام عن المستوى العادي بشكل ملحوظ"، كتب الملازم أول في الجيش الأميركي، جيه. أر. تشايلدس، في الشيفرات العسكرية الألمانية من شباط/فبراير إلى تشرين الثاني/نوفمبر من العام *1918* .

وفي الحرب العالمية الثانية، فاق اليابانيون الأميركيين براعةً من خلال ابتكار حركة اتصالات لاسلكية مضلِّلة. فقبل الهجوم على بيرل هاربر، نقل اليابانيون إلى الشاطئ العاملين على أجهزة الاتصال اللاسلكي الراصدة

للطائرات، مما أقنع الأميركيين بأن الأسطول الياباني ما يزال راسياً.

لقد تعلّمت الولايات المتحدة الدرس. ففي العام 1942، أنشأت مجموعة لتحليل حركة الاتصالات مكرَّسة لدراسة الرسائل اليابانية في المحيط الهادئ. وبالرغم من عدم فك الشيفرات اليابانية حتى العام 1943، تمكنت وحدة تحليل حركة الاتصالات من "تحديد مواقع الجنود، وسلسلة القيادة، وترتيب المعركة".

في الخمسينات، نقلت وكالة الأمن القومي تحليل حركة الاتصالات من البطاقات المثقوبة إلى أجهزة الكمبيوتر. كان هدف محلّل حركة الاتصالات "رسم صورة عن المستهدَف"، وفقاً لدراسة أجرتها وكالة الأمن القومي عام 1982. "عندما يَعرف السلوك العادي للمستهدَف، يكون في وضع يسمح له باكتشاف الاختلافات وإبلاغ معالِجي المعلومات الاستخباراتية بها".

يمكن لتلك "الشواذات" الكشف عن كثير من المعلومات. ففي العام 2004، كشف حزب الله في لبنان ما يقدّر البعض أنه مكان مئة جاسوس - من بينهم عملاء سي آي أيه ربما - من خلال تمييز هواتف محمولة نادراً ما استُخدمت، أم استُخدمت فقط، من مواقع محدَّدة لمدة قصيرة من الزمن.

á á á

كلما عرفتُ المزيد عن شبكات تعقُّب الهواتف المحمولة، ازدادت استحالة تمكّني من الفرار منها.

كان الحل البديهي ترك الهاتف في المنـزل، ولكن كوني والدةً لصغيرَين، شعرت بأن عدم إمكانية الاتصال بـي عبر هاتفي المحمول في أي وقت من النهار أو الليل هو أمر غير مسؤول - ووافَق زوجي. لذلك قررت أن الأمر التالي الأفضل شراءُ هاتف "خادع". فالهواتف الخادعة عبارة مستخدَمة للهواتف المسبَقة الدفع التي تُستخدم لفترة قصيرة ومن ثم يتم التخلي عنها.

والهواتف الخادعة ليست خياراً مثالياً - بقدْر كافٍ من الجهد، يمكن للمحقِّقين ربط هاتف خادع بهويّتكم استناداً إلى أنماط اتصالاتكم أو موقع هاتفكم. ولكن شراء هاتف دون الإفصاح عن اسمكم يعني أنه عندما تُباع بياناتكم أو تُجمَع من قِبَل الحكومة، على الأقل، يتطلب الأمر مرور بعض الوقت قبل أن يتمكن المحقِّقون من ربط المعلومات بهويّتكم الفعلية.

لذلك، قررت القيام بمحاولة. فأثناء إجراء بحث عن الهواتف، وجدت أنني بحاجة إلى هواتف أندرويد لأن تطبيقات حماية الخصوصية متوافرة

لهذه الهواتف أكثر من توافرها للـآي فون. كان اختيار موفر خدماتِ الاتصال عبر الهواتف المحمولة أكثر صعوبة. فأيٌّ منهم لا يعرض خيار عدم تخزين أية بيانات. ووفقاً لمستند عن إنفاذ القانون حصل عليه الاتحاد الأميركي للحريات المدنية، يخزّن معظم موفّري الهواتف المحمولة سجلات مفصَّلة لعامَين تقريباً، وتقوم أيه تي أند تي بتخزينها لما بين خمس وسبع سنوات. في النهاية، قررت أنهم متساوون في الأساس، باستثناء أيه تي إند تي، لذلك اخترتُ نظاماً رخيصاً مُسبَق الدفع من فرجين موبايل.

إن الممارسة الفضلى أثناء شراء هاتف "خادع" هو الدفع نَقداً وشراؤه من متجر بعيد عن المنـزل. لذلك، سحبتُ مبلغ 200 دولاراً نقداً وقصدتُ متجراً في وسط مدينة مانهاتن - غير معروف بشكل ملائم كما يبدو - لشراء الهاتف. فأصرّت الموظفة الكتابية المدقِّقة على قيامي بالضغط على عدد قليل من الشاشات بعد تمرير بطاقة الائتمان الممغنطة داخل جهاز قارئ، عِلماً أنني دفعت نَقداً. وعرضت عليّ بعد ذلك حَسماً مضموناً إذا أدخلتُ معلوماتي الشخصية إلى الجهاز. ومن ثم، عرضت عليّ خصماً على الهاتف أيضاً إذا أدخلتُ المعلومات. فرفضتُ باحترام، ولكن رفضي المتكرر تقديم معلومات شخصية حملني على الشعور بأنني مجرمة. عندما غادرت المتجر وهاتفي في حقيبتي، شعرت كما لو أنني أحمل بضاعة مهرَّبة. فرفعت نظري لأتحقق مما إذا كان بإمكاني رؤية كاميرات مراقبة فورية قرب الباب. لقد تمنيت لو كنت أعتمر قَلنسوّة بيسبول.

كان يُفترض بتوقفي التالي أن يكون لشراء بطاقة شهرية مُسبَقة الدفع من متجر آخر تحتوي على سيولة نقدية. ولكنني عرفت بأنني سأُغفل حداً زمنياً أقصى في نهاية المطاف إذا اتكلت على السيولة النقدية. فقصدت المنـزل واستخدمت بطاقة ائتمان آيدا تاربيل لأشترك في خدمة شهرية مسبَقة الدفع من فرجين موبايل.

بالرغم من كل شيء، لا يتمثل هدفي بأن أكون مجهولة الهوية تماماً بل حمل المتعقّبين على العمل بكدّ أكبر.

á á á

لم أصرّح برقم هاتفي الخادع، بل أعطيت زوجي، حاضنة أطفالي، وعدد قليل من الأصدقاء، رقم هاتف ماسك مي الذي اشتريته من إيْبِن. لقد أعددته كي ترسَل كل الاتصالات بالرقم المخفيّ إلى هاتفي الخادع.

ولكن المشكلة تمثّلت بعدم تمكني من إجراء اتصالات أو توجيه رسائل نصّيّة من خلال الرقم المخفيّ. كان باستطاعتي تلقّي رسائل نصّيّة عبر الرقم

المخفيّ، ولكن إجابتي على الرسائل النصّية ستكشف عن رقم هاتفي الخادع.

كنت انحرف إلى منطقة رمادية من القانون؛ من غير القانوني إخفاء رقم هاتفكم بنيّة الاحتيال. ففي العام 2010، وقّع الرئيس أوباما على مرسوم الحقيقة في هوية المتصل ليصبح قانوناً، مما يجعل من غير القانوني "تعمّد نقل معلومات شخصية مضلِّلة أو غير دقيقة عن المتصل بنيّة الخداع، إلحاق الأذى، أو الحصول على أي شيء ذات قيمة بطريقة لا أخلاقية".

بالطبع، لم أكن أخطط لإخفاء رقم هاتفي بنيّة الاحتيال أو إلحاق الأذى، ولكن من المحتمل أن تكشف اتصالاتي عن هويّتي حتى ولو نجحتُ في إخفاء رقمي. ناظرةً إلى سجل المكالمات على هاتفي العادي، أدركت أنه يمكن التنبّؤ إلى حد كبير بنماذج اتصالاتي (المُملّة). فكل يوم أتصل بزوجي نحو الساعة السادسة مساءً. وكل يوم بعد يوم، أتحدث إلى أمي، شقيقي، وعدد قليل من الأصدقاء. وتندرج كل اتصالاتي الأخرى في إطار ذلك الخط الكفافي الأوسع.

لذلك، قررت استخدام الهاتف الخادع لاتصالات العمل فقط. فاصطحبته في رحلة عمل إلى العاصمة واشنطن، واستخدمته بشكل حصري مدة ثلاثة أيام من الاجتماعات واللقاءات. لقد اصطحبت هاتفي الشخصي أيضاً، آي فون، واحتفظت به في غرفة الفندق، وأطفأته، متعهّدةً باستخدامه للاتصالات الشخصية فقط.

ولكن، كان من الصعب، في نهاية المطاف، إبقاء الهاتفَين منفصلَين. لقد وجدت نفسي عالقة في زحمة مرور في سيارة أجرة وأردت الاتصال بالمنـزل، لذلك استخدمت الهاتف الخادع. وعندما عدت إلى غرفة الفندق، نسيت إطفاء الهاتف الخادع كي أفصل بين موقعَي الهاتفَين.

بدأت أفهم عما كان مايك بيري، الذي أعلن نفسه " نباتياً متشدداً حيال الرَّقابة"، يتحدث عندما قال إن استخدامه هواتف مختلفة لشبكات تواصل اجتماعي مختلفة ألحقت الضرر بقدرته على إقامة علاقات وثيقة.

á á á

وحمّلتُ هاتفي الخادع تطبيقاتٍ لحماية الخصوصية أيضاً. لقد كرهتها على الفور تقريباً.

فلتصفّح الويب، تعيّن عليّ تثبيت برامج إخفاء الهوية الذي يرسل حركة اتصالاتي على الويب عبر أجهزة كمبيوتر في مختلف أنحاء العالم. بتلك

الطريقة، لا تعرف مواقعُ الويب التي أزورها عبر هاتفي مكاني. (بالطبع، ما يزال مزوّدي بالهاتف المحمول يعرف مكاني، أو على الأقل مكان آيدا تاربيل).

لقد اعتقدت أن برنامج إخفاء الهوية - تور - بطيء عندما استخدمته لإعداد حسابات لآيدا عبر الإنترنت على جهازي الحضني. ولكن الأمر أسوأ بكثير على هاتفي. كان بطيئاً على نحو متجمّد وأتلفَ بطاريتي. لقد تطلّب الأمر استخدامي ساعةَ توقيت لأكتشف أن التوجيه إلى كافة أنحاء العالم من خلال شبكة تور لم يُفعَّل إلا بعد أربع عشرة ثانية، ومن ثم تطلّب الأمر ست ثوانٍ أخرى لإطلاق متصفّح الويب الذي يوجّه البيانات عبر تور، وأخيراً، مضت ثلاث وأربعون ثانية قبل إجراء بحث بسيط عبر الويب عن "الطقس في نيويورك". ككل، تطلّب الأمر أكثر من دقيقة للبحث عن الطقس.

بالمقارنة، تطلب إطلاق متصفّح الويب من غوغل، وكروم، والبحث عن "طقس نيويورك" تسع ثوانٍ على هاتفي آي فون.

قالت لي هارلو هولمز، رئيسة ما وراء البيانات في غارديان برودجكت التي تصنع برنامج تور الرسمي لأندرويد، إن تصفّح الويب بواسطة تور يأخذ مزيداً من الوقت لأنه يقوم بمزيد من "الوثبات" بين هاتفي وموقع الويب الذي أزور. "هناك بالتحديد تنازل عن إحدى ميزتَي السرعة والغُفلية أثناء استخدام تور من أجل الحصول على أخرى"، قالت لي.

في النهاية، أقلعتُ عن استخدام تور وثبّتُّ تطبيق داك داك غو على هاتفي. تطلّب إطلاق داك داك غو والبحث عن "طقس نيويورك" خمس عشرة ثانية فقط - أبطأ من غوغل ولكنه ليس طويلاً ومُمِلاً مثل تور.

بالرغم من ذلك، أدركت أنني كنت أتجنّب تماماً إجراء أبحاث على الويب. ذات مساء، عندما التقيت صديقتي لتناول مشروب، قررنا الحصول على شيء ما نأكله. ولكن من أين؟ فكما يفعل الناس اليوم، أخرجتْ كل منا هاتفها المحمول. لقد بحثتُ في داك داك غو عن توصيات متعلقة بالمطاعم، ولكن بما أنه لا يعرف موقعي، فقد تطلّبه الأمر بعض الوقت للحصول على الإحداثيات الصحيحة. وبينما كنت أُدخل عبارة "مطاعم مكسيكية حديقة ميدان ماديسون العامة مدينة نيويورك"، عثرت صديقتي على مطعم قريب.

مغتمّة، اتصلتُ بموكسي مارلينسبايك، المطوِّر الذي وضع تطبيقات الرسائل النصّية الآمنة والاتصالات الهاتفية التي أستخدم (هي سهلة

الاستخدام نوعاً ما، في الواقع). فمارلينسبايك هو أحد المتسللين إلى الهواتف المحمولة، وهو الأكثر عمقاً في التفكير وتمتعاً بالموهبة هناك. لقد سألتُه عن سبب صعوبة استخدام كل أدوات إخفاء الهوية هذه.

"لا وجود في الواقع لسوقٍ برامج تحافظ على خصوصية المستهلك"، قال لي مارلينسبايك. هو يتلقى التمويل، من خلال المِنَح، مع مطوِّرين آخرين لهواتف محمولة تميل إلى حماية الخصوصية - مثل غارديان برودجكت.

قال مارلينسبايك إنه كان يحاول اجتذاب مبرمِجين موهوبين يمكنهم الذهاب في ظروف أخرى للعمل في شركات في المرحلة الأولى من عملياتها، في سيليكون فالي. واستخدم مِنحته الأخيرة كي ينقل فريقاً من المطوِّرين جوّاً إلى هاواي لقضاء أسبوعٍ برمجة على الشاطئ. ولكن مارلينسبايك يعمل على نطاق ضيّق. إن تطبيقَيه - رِدفون (RedPhone) وتكست سيكيور (TextSecure) - يعملان على أندرويد فقط، ومعظم أصدقائي يستخدمون آي فون، لذلك لا يمكنني تشفير اتصالاتنا بواسطة تطبيقاته.

فضحك عندما أخبرته عن نضالي مع تور. "كلما استخدمتُ تور وهو سريع، أُصبح عصبيّ المِزاج لأنني أسأت تركيبه"، قال. "لا فائدة من كل هذه الأشياء. كل أدواتنا مروِّعة. علينا الاعتراف بذلك".

á á á

في غضون ذلك، دأبت صناعة تعقُّب الهواتف المحمولة على بناء أدوات أكثر تطوّراً لتعقُّب المواقع.

إن السباق في القطاع الخاص لوضع خريطةٍ لموقعِ كل جهاز في العالم بدأ بممارسةٍ تدعى "البحث عن شبكات واي - فاي انطلاقاً من مركبة متحركة". قمت بهذا البحث للمرة الأولى في دِنفِر عام 2002 مع بعض تقنيّي شركةِ كَبلاتٍ للإرسال التلفزيوني والاتصالات عبر الهاتف والإنترنت قدّموا لي عرضاً عن كيفية القيام بعملية البحث. لقد تنقلنا في الأنحاء بسيارة، وأبقى التقنيّ في مقعد الركاب جهاز كمبيوتر حضني مشغَّلاً، وعلى جهازه برنامج يمسح المناطق المحيطة بحثاً عن شبكات واي - فاي. فكلما عثرنا على جهاز غير مشفَّر يؤمّن ولوج الإنترنت عبر شبكة واي - فاي، توقّفنا وراقبنا حركة الاتصالات عبر الإنترنت تتدفق عبر شاشة جهازه. لم نقرأ أيّاً من المعلومات، ولكن كان بإمكاننا القيام بذلك.

عام 2003، إمتهنت شركة في بوسطن تدعى سكايهوك البحثَ عن شبكات واي - فاي انطلاقاً من مركبة متحركة. لقد نشرت سكايهوك سيارات

ماسحة للأسماء ولطول إشارات الأجهزة التي تؤمّن ولوج الإنترنت عبر شبكات واي - فاي. لم تقرأ سكايهوك أيّاً من حركة الاتصالات عبر الواي - فاي، بل كان مجرّد وضع خرائط لمواقع هذه الأجهزة حول العالم. "اعتقد الناس أننا مخبولون في السنوات الأربع أو الخمس الأولى"، قال مؤسس سكايهوك، تِد مورغان.

ولكن رهان سكايهوك عاد عليها بالفائدة. لقد ثَبُت أن أجهزة ولوج الإنترنت عبر شبكات الواي - فاي كثيفة بما يكفي لدرجة تمكُّنها في غالب الأحيان من توفير معلومات دقيقة عن المواقع. إليكم طريقة عملها: يلاحظ هاتف محمول شبكات الواي - فاي من حوله، ويضع بيانات عن موقعها في قاعدة بيانات سكايهوك، ويستخدم تلك المعلومات لتقدير موقع الهاتف.

غالباً ما أعتبر العثور على موقع عبر الواي - فاي إضافةً تحسينية إلى الوسائل السابقة - من خلال تقنية المسح بالتثليث بين أبراج الهاتف المحمول أو أقمار نظام تحديد المواقع العالمي الصناعية، التي يمكن للمباني أو لعقبات أخرى صدّ الإشارات.

سرعان ما واجهت سكايهوك منافسة. ففي العام 2007، شرعت غوغل باستخدام سياراتها ستريت فيو للبحث عن شبكات واي - فاي وبناء قاعدة بياناتها الخاصة. وبعد الإمساك بسياراتها تجرف كلمات مرور البريد الإلكتروني ومعلومات شخصية أخرى من خلال هذه العملية، أوقفت غوغل عملية البحث وبدأت باستخدام هواتف أندرويد لجمع معلومات عن إشارات واي - فاي.

في العام 2010، شرعت أبل أيضاً ببناء قاعدة بياناتها عن شبكات الواي - فاي، مستخدمةً أجهزة الآي فون لجمع معلومات. في الأساس، كانت غوغل وأبل تستخدمان هواتف زبائنهما لإجراء عملية البحث. (هل ندعو الأمر "هوتفة الحرب"؟)

في غضون ذلك، كانت تطبيقات الهواتف المحمولة والمعلنون يخوضون حرباً عبر الهواتف أيضاً. ففي العام 2010، اختبر فريق استقصاء الخصوصية الذي أقود في وول ستريت جورنال 101 تطبيق للهواتف الذكية (هواتف محمولة مماثلة للكمبيوترات الشخصية في المهام) ووجد أن 47 منها يبثّ موقع الهاتف المحمول إلى خارج الشركات. لم ينجم عن خمس وأربعين تطبيقاً سياسات في شأن الخصوصية تُنبئهم بكيفية تصرّفهم بالمعلومات.

لقد تسابقت شركات في المرحلة الأولى من عملياتها على بناء تجهيزات يمكنها سحب إشارات واي - فاي من هواتف المستخدمين أثناء مرورهم

بجانب موقع ما. ووضعت بعض الشركات التجهيزات في مراكز تسوّق لتعقُّب الزائرين، حتى إن شركة تسويق لندنية، تدعى رينيو، ثبّتت أجهزة تعقُّب هواتف ذكية في صناديق تدوير القُمامة لمراقبة الناس أثناء مرورهم بجانبها. (كفّت الشركة عن هذا الإجراء بعد طلب المنطقة المالية إيقاف عملية الجمع).

قال كافيه ميماري، المدير التنفيذي الأول لرينيو، إن النظام حقق نجاحاً لأن 80 بالمئة من اللندنيين يتركون شبكات الواي - فاي مشغَّلة عندما يغادرون منـزلهم أو مكتبهم. "الفرص متوافرة للإيقاع بكم في النهاية إذا لم نركم في اليوم الأول، الثاني، أو الثالث"، قال. "نحن بحاجة إليكم لإبقاء شبكة الواي - فاي مشغَّلة مرة واحدة فقط".

فجأةً، لم يَعُد موفِّرو خدمات الاتصال عبر الشبكات اللاسلكية يحتكرون مواقع مستخدمي الهواتف المحمولة. لم يكن هناك أي سبب يمنعهم من بيع البيانات أيضاً.

عام 2012، أطلقت فريزون شركة تدعى برِسيجن ماركت إينسايتس لبيع بيانات عن "الفئة العمرية، الجنس، والرموز البريدية، لمعرفة أماكن إقامة، وعمل، وتسوّق" مستخدمي هواتفها المحمولة، إضافةً إلى معلومات عن عادات الأجهزة المحمولة "بما في ذلك زيارات عناوين صفحات الويب، وتحميل تطبيقات واستخدامها، وميولٍ تصفّحية، وسواها". وفي العام 2013، قالت أيه تي إند تي إنها ستشرع أيضاً ببيع معلومات عن مواقع المستخدمين وعادات تصفّح مواقع الويب. وأصبح تعقُّب مواقع الناس من خلال الهواتف فرصة لتجارة رائجة ولّدت مؤتمرات مثل معلومات عن المواقع في العاصمة واشنطن، وقمة الجِيوويب في مدينة نيويورك، وقمة تجارة المواقع في سان هوزيه، كاليفورنيا.

في مؤتمر الإشارات في شيكاغو عام 2012، وصفت شركة لتحليل المواقع، تدعى جيه آي واير، المعاني الضمنية التي جمعتها من النِّبذات التي وضعتها عن سلوك أكثر من سبعمئة مليون جهاز. "إن مكان وجودكم يُنبئ بأكثر مما تُنبئ به أية معلومة أخرى"، قال ديفيد ستاس، رئيس جيه آي واير.

á á á

بالطبع، تقول كل شركات تعقُّب المواقع إن البيانات التي تجمعها مجهولة الهوية. فكل ما يقومون بجمعه هو مجموعة أرقام مساوية لرقم متسلسل لهاتفكم.

"لا يمكننا تلقّي، ولن نتلقى، أية معلومات مرتبطة بأسماء، عناوين، أرقام هاتف، عناوين بريد إلكتروني، ألخ"، كتب ويل سميث، المدير التنفيذي الأول لشركة المواقع، أوكليد، في رسالة للسيناتور آل فرانكن عن ولاية مينيسوتا، الذي قدّم مشروع قانون يُلزم الشركات بطلب الإذن قبل تعقُّب مواقع الناس.

تساعد أوكليد الباعة بالمفرّق على تحديد هوية المتسوّقين عبر إشارات الواي - فاي التي تبثّها هواتفهم المحمولة، وعبر عناوين أم أيه سي (ضبط ولوج وسائل الإعلام - Control Access Media) وهي أدوات تحديد فريدة للهوية خاصة بالهواتف شبيهة نوعاً ما برقم متسلسل. فمنذ إطلاقها عام 2011، تقول أوكليد إنها عدّت خمسين مليون جهاز في متاجر زبائنها.

وقال سميث إنه بجمع معلومات مجهولة الهوية فقط، تسعى أوكليد إلى "حماية خصوصية المستهلك". ولكن الحقيقة تتمثل بأن الموقع هو أحد أجزاء البيانات الأكثر كشفاً عن الأشخاص. ففي العام 2013، درس باحثون في معهد ماساشوستس للتكنولوجيا، وجامعة لوفان الكاثوليكية في بلجيكا، خمسة عشر شهر من بيانات مواقع 1,5 مليون شخص. لقد وجدوا أن خمسة أمثلة عن مواقع أشخاص في زمن محدَّد كافية لتحديد هوية 95 بالمئة من الأفراد الذين تناولتهم الدراسة. "آثار حركية الناس فريدة إلى حد كبير"، كتب الباحثون. "إن بيانات الحركية هي من بين البيانات الأكثر حساسية التي تُجمَع في الوقت الحاضر".

ويمكن التنبّؤ بالموقع أيضاً. لقد وجد باحثون في مايكروسوفت أن بالإمكان استخدام بيانات المواقع للتنبّؤ بدقة عن مكان تواجد الناس في المستقبل. مستخدمين بيانات من أكثر من ثلاثمئة متطوّع، وجدوا أن باستطاعتهم التنبّؤ بمكان تواجد الناس في المستقبل. كانت أيام الأربعاء الأسهل لإجراء التنبؤات، ونهايات الأسبوع أكثرها صعوبة. "في حين يكون موقعكم في المستقبل البعيد مستقلاً إلى حد كبير، وبصورة عامة، عن موقعكم الأحدث عهداً"، كتب الباحثون، "من المحتمل أن يكون متنبّئاً جيداً لموقعكم بعد أسبوع واحد".

لقد بدا هذا الأمر بعيداً جداً عن الغُفلية. فهم لا يعرفون هويّتي ومكان تواجدي فحسب، بل يعرفون أيضاً أين سأكون بعد أسبوع.

á á á

للحدّ من تتبّع المواقع، أطفأتُ الواي - فاي على هاتفَيّ المحمولَين (العادي والخادع) وتعهّدتُ بعدم تشغيلهما أبداً. وأوقفتُ خدمات تحديد

المواقع على كلا الهاتفَين أيضاً. حتى إنني غيّرت اسم جهازي المنـزلي لنقل رِزم بيانات عبر الواي - فاي، مُضيفةً - nomap إلى آخر الاسم بهدف عدم الاشتراك بقاعدة بيانات خدمة المواقع التابعة لغوغل.

وحدّدتُ أيضاً هوية ثمانٍ وخمسين شركة ظهرت في آليّة تعقُّب المواقع على الهاتف المحمول - تتراوح بين معلنين، وهواتف تعقُّب الأشخاص في صناديق تدوير القُمامة، وموفِّري خدمات الاتصال عبر الشبكات اللاسلكية. من بين تلك، سبع فقط عرضت خيارات عدم الاشتراك.

كنت ما أزال غير بعيدة جداً عن شبكة تعقُّب المواقع. فقررتُ الشروع في إطفاء هاتفي المحمول في غالب الأحيان كي لا يتم تعقُّب موقعي باستمرار. وفكرتُ ملياً في وضعه في صيغة الطائرة، ولكنني لم أشأ (مرة أخرى) تكبّد عناء التلهّي بالإعدادات.

لقد اعتبرتُ أنه من الأسهل وضع هاتفي المحمول في حقيبة تصدّ الإشارات. تُدعى هذه الحقائب "أقفاص فاراداي" تيمّناً بالعالِم الإنكليزي مايكل فاراداي الذي اكتشف أن تبطين غرفة بمعدن يصدّ الإشعاع الكهرمغناطيسي. مذاك الحين، استُخدمت أقفاص فاراداي في الرعاية الصحية، والقوات المسلحة، وأماكن أخرى حيث يريد الناس منع التشويش الكهرمغناطيسي الذي تتسبّب به أجهزتهم.

عندما أخبرتُ جون ستراوشز، عميل السي آي أيه السابق، وأردت قفص فاراداي لهاتفي، ضحك وأطلعني على خدعة بسيطة يمكن استعمالها عند الحاجة. "يمكنك استخدام رُقاقة ألومنيوم ببساطة!" قال لي.

ونجح الأمر، في الواقع. لقد لففتُ هاتفي الخادع بورق فضّي وحاولتُ الاتصال به. لم يرنّ. لذلك، رميت هاتفي الخادع الملفوف برُقاقة ألومنيوم في حقيبة يدي وخرجتُ لإجراء مقابلات في نيويورك طوال اليوم.

لقد أبقيتُه في حقيبة يدي ولم أفضّ الرُّقاقة عنه إلا بين اللقاءات عندما لا أكون محطّ الأنظار. وتطلّبه الأمر دقائق قليلة كي يتّصل بالبُرج ويحمّل أية نصوص، ورسائل بريد إلكتروني، واتصالات مُغفَلة. راضيةً، لففتُه ثانيةً ورميته في حقيبة يدي.

في نهاية اليوم، كان الورق الفضّي متجعّداً وممزَّقاً في أماكن قليلة، وباتت عملية إعادة لف الهاتف تماماً أكثر صعوبة أثناء محاولتي رَقع الثقوب. لقد بدت على زميلي، جريمي سينجر - فاين، ملامح تعرّضه لصدمة عندما رأى بِدعة ورق الفضّة. "لديّ حقيبة فاراداي لا أستخدمها"، قال لي. "هل تريدينها؟"

بعد أيام قليلة، أحضر لي جريمي حقيبة فضيّة جميلة مع آليّة إغلاق فِلكرو، واتّسعت الحقيبة لهاتفي تماماً - ولم تخترقها الاتصالات. لقد أحببتها.

جعلني ورق الفضة أبدو كشخص مجنون، ولكن حقيبة فاراداي جعلتني هادئة وواثقة؛ أراد كل أصدقائي حقيبة مماثلة.

á á á

بالطبع، كنت فضولية في شأن مبتكِر حقيبة فارادي. لذلك عرفّني جريمي بآدام هارفي.

التقيتُ وآدام لتناول القهوة في وسط المدينة. طويل القامة وهزيل، أخبرني آدم بأنه مهتم بالتقارب الحاصل بين الموضة ومكافحة الرَّقابة عندما كان في برنامج تخرُّج في جامعة نيويورك عام 2009.

كان لباسه الأول المدعوّ انسلالياً "جهازاً مضاداً للباباراتسي" يستجيب لومضة آلة التصوير من خلال إطلاق ضوء ساطع يُتلف الصورة الفوتوغرافية الملتقَطة. "كنت على ثقة بضرورة امتلاك الأشخاص الذين تُلتقط لهم صور فوتوغرافية من قِبَل الباباراتسي وسيلةً لإطلاق ومضة مضادة"، قال لي. لم يحقق الجهاز رواجاً، ولكنه حمله على التفكير في طرق أخرى لحماية الخصوصية علَناً. بالنسبة إلى أُطروحة الماجستير، ابتكر مجموعات شَعر وأساليب تبرّج يمكنها إحباط برامج اكتشاف الوجوه. ولكن النظام لم يكن عملياً: يقتضي العديد من الأساليب وضع شعر فوق وجوهكم أو تلوين أجزاء من وجوهكم بالأسود.

في النهاية، وقع على فكرة بناء أقفاص فاراداي لأجل الهواتف المحمولة. في البداية، حاول ابتكار سِروال يحتوي على جَيب مصنوع من القطن وخيوط فضيّة يمكنها صدّ إشارات الهاتف المحمول. ولكنه سرعان ما أدرك أنه من غير المنطقي وضعه مبيَّتاً في السروال. لذلك، شرع بالعمل على كُمّ للهاتف المحمول - يدعوه جَيباً غريباً.

إن الذي أضعه في حقيبة يدي، قال، نموذج أوّلي. هو يقلّص قوة إشارة برج هاتف محمول بنسبة 80 دسيبل. "أنتِ بحاجة إلى تقليص يزيد عن 95 دسيبل لأجل حماية كاملة"، قال. والجهاز الجديد الذي سيُطلقه يقلّص قوة الإشارة بنسبة 100 دسيبل. "أرى أن الخصوصية لن تُمنح لك على صورة قانون تماماً"، قال لي. "عليك أن تجعليه قابلاً للتسويق كي يتمكن الناس من إبداء رأيهم بواسطة المال".

á á á

لم أحصل على النتيجة المرجوّة حتى بعد إنفاق المال لحلّ المسألة.

كان رقم هاتفي المخفيّ وهاتفي الخادع مصدرَ تسلية، ولكن أيّاً منهما لم يحمِ موقعي أو شبكة اتصالاتي.

لقد نجحت عمليةُ وضعِ هاتفي المحمول في قفص فاراداي، ولكنها كانت بسوء ترك هاتفي في المنـزل؛ لم يكن بالإمكان الاتصال بـي حتى أقوم بإخراجه من الحقيبة.

كانت خبراتي في خصوصية الهاتف المحمول أكبر إخفاق لي.

الفصل الحادي عشر
اختيار عدم الاشتراك

عندما أخبرت شقيقي بأنني سأُزيل نِبذتي عن LinkedIn ، قال إنني مجنونة. "من خلال النِّبذة، سيتمّ تجنيدك لعملك التالي".

لم أكن أتحمّل رفض عملي التالي. فصناعتي - الصحف - كانت في سقوط حُرّ في الأساس. وحتى لو لم أكن بحاجة إلى عملي التالي في هذا العام، لن يمرّ وقت طويل حتى أصبح بحاجة إليه.

ولكنني لم أتمكن في الواقع من تبرير بقائي على LinkedIn ، نظراً إلى مدى تعريض شبكتي الاجتماعية للإفشاء. لقد سمحت لي إعدادات الخصوصية في LinkedIn بمنع الآخرين من رؤية "عمليات وصلي"، ولكن سياسة الخصوصية المتَّبَعة من قِبَله تشير إلى أن "الناس سيكون بإمكانهم على الدوام رؤية عمليات وصل مشترَكة".

يعني ذلك أنني إذا تشاطرت وإيّاكم صِلة LinkedIn ، يمكننا أن نرى صداقتنا تلك على الشاشات. يبدو آمناً، ولكنه لا يختلف كثيراً في الواقع عن قاعدة بيانات الاتصالات الهاتفية التابعة لوكالة الأمن القومي. إنها شبكة تعقُّب عملاقة للصِّلات القائمة بين الناس.

وهناك أيضاً هذا السطر المُقلق في سياسة LinkedIn المتعلقة بالخصوصية: "لا نؤجّر أو نبيع معلومات شخصية لا تنشرونها على LinkedIn ". أممم، أظنّ أنهم يبيعون كل المعلومات التي نشرتُها على LinkedIn ؟ تقول LinkedIn إنها لا تبيع معلومات شخصية لأطراف ثالثين، ولكنها تبيع بالفعل خدمات تسمح للمجنِّدين بالبحث عن معلومات الأعضاء والاتصال بهم.

وأعرّض كل هذه الأمور للإفشاء مقابل ماذا؟ نادراً ما أستخدم LinkedIn . كانت لدي 220 عملية وصل، و27 رسالة غير مقروءة، و570 دعوة بانتظاري. وحتى ولو حاول مجنِّد الوصول إليّ عبر LinkedIn ، لَما لاحظتُ ذلك على الأرجح.

ولكنني أُغويت بفكرة إمكانية قيامي باستخدام LinkedIn ذات يوم، وبأنه قد يساعدني للحصول على عمل جديد عندما أكون في مأزق. هذا ما يدعوه عالِم الاقتصاد السُّلوكي دان أريلي "دافعنا غير المنطقي الذي لا يقاوَم لإبقاء الأبواب مفتوحة".

يصف أرييلي اختباراً أجراه ومارس فيه الطلاب لعبة فيديو تُظهر ثلاثة أبواب - أحمر، أزرق، وأخضر. ويفتح كل باب على غرفة وهمية حيث يمكن للّاعبين جني مبلغ معيّن من المال بنقرة واحدة. يتمثل هدف اللعبة بجني أكبر قدْر من المال بعدد محدَّد من النقرات.

عندما بدأتِ اللعبة، اتّضح أن أولئك اللاعبين الذين اختاروا غرفة ولازموها حققوا أفضل نتيجة اقتصادية. ولكن اللاعبين واصلوا إبقاء كل الأبواب مفتوحة حتى عندما شُرحت لهم الجوانب الاقتصادية بوضوح. "ما يزالون لا يُطيقون رؤية باب مُغلَق"، كتب أرييلي. "ما تزال لديهم الحماسة اللامنطقية نفسها لإبقاء أبوابهم مفتوحة".

تتمثل المشكلة بأن البشر يكرهون التعرّض للخسارة، حتى ولو خسروا شيئاً غير هام. لقد وصف هذا الأمر شعوريَ تماماً حيال التخلّي عن LinkedIn . لقد استحوذ على عقلي طوال أشهر، واستشرت خبيرَين في كيفية الاستفادة من محرك البحث إلى الدرجة الفضلى لأعرف ما إذا كان التخلّي سيُلحق الأذى بنتائج بحثي؛ (لن يُلحق الأذى). وتحدّثتُ إلى أصدقاء والعائلة في شأن ما إذا كان يُفترض بـي سحب السِّدادة.

كل ذلك لأجل موقع على الويب لم أسجّل دخولي إليه طوال عامَين؛ موقع على الويب تم التسلّل إلى كلمات مروره وتبيّن أنه لم يتم الاحتفاظ بها بالطريقة الملائمة؛ موقع أرسل لي قدْراً مزعجاً من البريد الإلكتروني؛ موقع لم أكن بحاجة فيه إلى وصف إنجازاتي المهنية لأنني أملك سيرة كاملة على موقعي الخاص على الويب. نحن نتكلم عن خوف غير منطقي من التعرّض للخسارة.

أخيراً، اتخذتُ خطوة جريئة وأغلقت حسابـي. أفاد موقع LinkedIn إنه سيزيل الطابع الشخصي عن أية مدوَّنات مرتبطة بحسابـي في غضون ثلاثين يوماً بعد إغلاقي الحساب.

ففي ثقافة تشهد قيام الناس بإصدار أحكام على أحدهم الآخر من خلال آثارهم الرقمية بقدْر حكمهم على ما هم عليه في الواقع، يُعتبر اختيار عدم المشارَكة في تشاطر بياناتكم فعلَ إيمان. الآن، سيكون عليّ الثقة بأن المستخدِمين المستقبليين سيعثرون عليّ بطريقة أو بأخرى.

á á á

إن اختيار عدم المشارَكة في سوق البيانات الشخصية هو تدرّب على الثقة.

في العالم الرقمي، تساعدنا نِبذاتنا على مواقع مثل LinkedIn وفيسبوك

على توطيد الثقة بأشخاص لم نلتقِهم أبداً. فقوة شبكات التواصل الاجتماعي تتمثل بأن "صِلاتكم" أو "أصدقائكم" يصلحون ليكونوا مُصادَقةً ضمنية على أمانتكم. "إن العرض العلَني للصِّلات هو تثبُّتٌ مُضمَر من الهوية"، كتبت الباحثتان جوديت دوناث ودانا بويد في مقالة لهما عن شبكات التواصل الاجتماعي.

من الأسهل اختبار إثبات الثقة عندما تلتقي أحدهم شخصياً. لقد وجد العلماء أن الناس يُطلقون أحكاماً دقيقة على نحو مفاجئ عن أحدهم الآخر في غضون ثلاثين ثانية، ولكن ذلك الوقت الإضافي لا يحسّن في العادة دقة تقديراتهم. عبر الإنترنت، يملك الناس أدوات أقل تساعدهم على تقدير الثقة. فالصور الفوتوغرافية على الإنترنت مضلِّلة بشكل مستقبَح، ويمكن تزييف أعياد المَولد، وتصل رسائل البريد الإلكتروني كما لو أنها مرسَلة من مصرفكم ولكنها تكون موجَّهة في الواقع من مجرم.

لقد قامت دوناث، وهي خرّيجة جامعية تواصل دراستها في مركز بيركمان للإنترنت والمجتمع في هارفارد بموجب منحة دراسية، بعمل خلاّب يتمثل بمقارنة مسائل الثقة عبر الإنترنت مع المشاكل التي تعاني منها الحيوانات أثناء التفريق بين الإشارات الصادقة والإشارات المخادِعة. على سبيل المثال، تأمّلوا بيَراعة فوتوريس "المرأة القاتلة" التي تُحاكي سلوك أُنثى يَراعة فوتينوس وتُغوي ذكَر فوتينوس، وتهاجمه، وتلتهمه. هو مثال عن الإشارة المخادعة.

من جهة ثانية، تأمّلوا بقرنَي أيِّل كبيرَين. لا يمكن للحيوان تحمُّل قرنَين ضخمَين دون أن يكون كبيراً وقوياً. "لا يحتاج المنافسون المحتمَلون أو القُرناء إلى اختبار قوة الأيّل مباشَرةً؛ يمكنهم النظر إلى حجم القرنَين ببساطة"، كتبتْ. هذا مثال عن الإشارة الصادقة.

تقول دوناث إن الصداقات عبر الإنترنت تُعتبر إشارات صادقة. فإذا كان شخص غير معروف صديقاً لصديقتي، يكون جديراً إذاً بقليل من ثقتي. ولكن الضغط الممارَس لابتكار هويّات عبر الإنترنت يولّد توتراً بين "الخصوصية والثقة". تساعد قصص عامة عن سلوك الأشخاص على توليد الثقة، قالت، "ولكن إذا كان يتعيّن القيام بكل شيء باسمكم الحقيقي، واجهتم الأثر المُرعِب أو جعلتم الناس عُرضة للأذى".

تعمل دوناث على طرقٍ لتصميم أنظمة تعزز الثقة بالأسماء المستعارة. "إذا أردتُ تحديد سعر مزيل رائحة الإبط، لست بحاجة إلى تشاطر اسمي الحقيقي مع عالم الإنترنت"، قالت. "الأسماء المستعارة هي أساس خصوصيتنا

عبر الإنترنت".

إكراماً لدوناث، ابتكرتُ نِبذة LinkedIn لأجل اسمي المستعار عبر الإنترنت، آيدا تاربيل. لا "صِلات" لآيدا، ولكنها تسمح لي بتسجيل دخولي إلى LinkedIn ورؤية ما يحدث هناك. لقد خفّف حضورها شعوري اللامنطقي بالخسارة بسبب تخليَّ عن LinkedIn .

á á á

أثناء استعدادي للانفصال عن فيسبوك، استشرتُ خرّيجة جامعية حديثة العهد، تدعى غابرييلا توديسكو، طلَباً للنُّصح.

لقد ألغت توديسكو حسابها على فيسبوك أثناء استراحة عيد الميلاد خلال عامها الجامعي الأخير في كارل بولي، سان لويس أوبيسبو. كانت تتخصص لتصبح مدرّسةً في المدارس الثانوية، ولم تشأ أن يرى مستخدِمها المستقبلي الصور الفوتوغرافية لزميلتها. "هناك صور - ولا سيما مع الكؤوس الحمراء - شديدة الخطورة في الواقع"، قالت لي. "يُخيفني الأمر حقاً، لذلك ألغيتُ الحساب برمّته".

كانت علاقة غابيـي بفيسبوك معقَّدة. ففي عامها الجامعي الأول، كانت وصديقاتها تُسجّلنَ دخولهنّ إلى فيسبوك في كل الأوقات، وتحمّلنَ صوراً لحفلات تظهرنَ فيها حاملاتٍ كؤوساً بلاستيكية حمراء.

عالقاتٍ في مناماتهنّ بدون سيارة، كانت وزميلاتها الثلاث في السكن مصابات بما دعته "إدمان غريب" على فيسبوك. وتابعت قائلة "لم يكن لدينا ما نقوم به باستثناء دخول فيسبوك وتحميل صور أو ملاحقة أشخاص".

على غرار مُدمنة حقيقية، كانت غابيـي تتخلّى بانتظام عن فيسبوك. ففي السنوات الثلاث الأولى من دراستها الجامعية، تخلّت عن فيسبوك لصالح لِنت (Lent). كانت تنقطع وصديقاتها عن فيسبوك لمدة أسابيع قليلة كما لو كان هناك قَدْر كبير من "الدراما" مع حبيب. "تغيّرين كلمة مرورك، وعندما أقرر العودة إلى فيسبوك، تعطينني كلمة المرور"، أبلغت غابيـي إحدى صديقاتها بهدف إرغام نفسها على الانقطاع الفجائي عن إدمانها.

كانت غابيـي تعرف طريقها حول إعدادات الخصوصية في فيسبوك ولم تسمح أبداً بفتح نِبذتها تماماً. لقد قيّدت ولوج صورها و"آرائها". وقبل التخلّي عنه، ألغت "وضعها على صعيد العلاقات" كي لا يصبح علَنياً عندما تتخلّى عن موقع التواصل الاجتماعي. وألغت أيضاً ألبوماتها وصورها

التعريفية التي لم تشأ لأصدقائها أن يروها.

مع ذلك، لم تكن واثقة من أن هذه الخطوات تفي بالغرض. ففي خريف عام تخرّجها، وأثناء بدئها بالتخطيط لمتابعة مهنة التدريس، شرعت بإخضاع آرائها المنشورة للرَّقابة وطلبت من زميلاتها في السكن الحصول على إذن قبل تحميل صور لها على فيسبوك. "كنا نقوم بالأمر معاً ونقول لا تحمّلنَ هذه الصورة"، قالت غايبـي. "إنه عمل جماعيّ جيد".

بحلول كانون الأول/ديسمبر، أدركت أنه من الأسهل لها التخلّي عن فيسبوك بدلاً من ضبطه. فبعد قراءة مقالة عن مدرّسة فقدت عملها بسبب صورة نشرتها على فيسبوك، قررتْ سحب السِّدادة.

وفي 24 كانون الأول/ديسمبر 2010، حمّلت كل صورها وألغت حسابها. لقد افتقدت الحساب في بادئ الأمر. "في البداية، شعرت كما لو أنني أريد الانتكاس قليلاً"، قالت لي. ولكنها سرعان ما بدأت بتقدير كل الوقت الذي طالبت باسترداده حق قدْره بعد كفّها عن التحقق من فيسبوك كل يوم وليلة.

عندما اتصلتُ بها بعد عام، كانت قد حصلت على عملها الذي حلُمتْ به، وأعربت عن غبطتها بسبب تخلّيها عن فيسبوك. كانت سعيدة بسبب عدم تمكن طلابها من دخول حسابها هناك.

بالطبع، كانت هناك لحظات افتقدتْ فيها فيسبوك. فعندما تُوفّيت إحدى زميلاتها في السكن في المدرسة الثانوية بشكل غير متوقَّع، لم يبلغها خبر الجنازة إلا بعد فوات الأوان على حضور الجنازة. "أدركتُ أنني لو كنت على فيسبوك، لَعَلِمتُ بالتأكيد موعد الصلاة الجنائزية"، قالت. "شعرت بأنني طائر يغرّد خارج السِّرب".

ولكن من جهة أخرى، إن عدم امتلاك حساب على فيسبوك يخدع المرء في شأن بعض المواعيد المحتمَلة. "جعلني هذا الأمر فريدة بعض الشيء وغامضة"، قالت.

á á á

عندما انضممت إلى فيسبوك في 26 حزيران/يونيو 2006، كان امتلاك حساب ببساطة يشير إلى ارتباطكم بجامعة نُخبوية. في ذلك الوقت، كانت العُضوية متوافرة فقط للمنتسبين إلى جامعات ومدارس ثانوية ولديهم عناوين بريد إلكتروني. في الواقع، لقد اشتركت في عنوان للخرّيجين من كلّيّتي بهدف الانضمام إلى فيسبوك ليس إلا.

كان دافعي صحافياً في المقام الأول: كنت أبحث عن كتاب يتناول

شبكة التواصل الاجتماعي ماي سبيس، وأريد فهم التواصل الاجتماعي عبر الشبكات. ولكنني استمتعت أيضاً بمصادقة مدرّس الرياضيات في المدرسة الثانوية الذي ألهمني، أو مصادقة الفتاة التي سرقت حبيبي في الكلّية. كنت أحب متابعة الصحافي الباكستاني الذي زار مكتبي ذات يوم بصفته زميلاً.

ولكن فيسبوك أساءت تكراراً إلى ثقة المستخدمين. لقد فقدتُ الصِّلة بعدد المرات التي غيّرتْ فيها الشركة إعدادات الخصوصية وأرغمتني على البحث في عمق قوائمها للمطالبة باستعادة السيطرة على بياناتي. ولكن الأمر جدير بإلقاء نظرة عن كثب على سياسات الخصوصية المُربِكة التي تتّبعها فيسبوك، وذلك لفهم كيفية نظرها إلى المستخدمين كبضاعة للبيع وليس كزبائن. يمكن فهم موقف فيسبوك بطريقة ما بما أن الزبائن لا يدفعون لقاء الخدمة، ولكنني لم أَعُد أرى مقاربتها جذّابة.

في العام 2007، أطلقت فيسبوك خدمة تدعى بيكون تهدف إلى مساعدة الناس على "تشاطر" نشاطاتهم التسوّقية عبر الإنترنت مع أصدقائهم. نتيجةً لذلك، عندما اشترى سين لاين خاتم ماس لزوجته على Overstock.com كهديةٍ مفاجئة بمناسبة عيد الميلاد، صُدم عندما وجد أن عملية الشراء نُشرت أوتوماتيكياً على حسابات أصدقائه الـ720، بمن فيهم زوجته. في العام 2009، وافقت فيسبوك على دفع 9,5 مليون دولار كتسوية لدعوى قضائية جماعية رُفعت ضد بيكون، وعلى إغلاق الخدمة.

ولكن بدلاً من التخلي عن فكرة توجيه مستخدميه إلى إعلانات لمنتجات مجانية، أحيا فيسبوك الفكرة في العام 2011 من خلال إطلاق منتَج يدعى قصص مَرعيّة يسمح للمعلنين بشراء حقوق إعادة نشر منشوراتِ مستخدمٍ ما وعرضها على أصدقاء ذلك المستخدم كإعلان. عام 2013، وافقت فيسبوك على دفع 20 مليون دولار كتسوية لدعوى قضائية جماعية رُفعت ضد قصص مَرعيّة. ولكن بدلاً من إلغاء المنتَج، أضافت فيسبوك ببساطة لغة جديدة إلى سياستها في شأن الخصوصية كي توضِح للمستخدمين أنه يحق لفيسبوك استخدام صور زبائنها ومنشوراتهم في الإعلانات. بمعنى آخر، كانت فيسبوك تشنّ حرب سنوات ست لتتمكن من تحويل أحاديث مستخدميها إلى إعلانات يمكن بيعها. (مذاك الحين، انضم غوغل إلى النِّزاع، مُطلقاً برنامجاً مماثلاً يدعى تعليقات مشترَكة يحوّل مراجعات المستخدمين، وتقديراتهم، وتعليقاتهم، إلى إعلانات).

ظهرت نقطة تحوّلي مع فيسبوك في كانون الأول/ديسمبر 2009 عندما

أدخلتْ فجأةً تعديلات على سياستها في شأن الخصوصية وتتضمّن كشف أسماء أصدقائي للجمهور التي كانت خاصة في السابق. كصحافية، أنا بحاجة إلى حماية مصادري. وكإنسانة، أفضّل ألا يكون هناك جمهور غير مرئيّ يراقبني أثناء اتصالي بأصدقائي.

غاضبةً، كتبتُ مقالة لوول ستريت جورنال تشير إلى خيانة فيسبوك للطبيعة الإسرارية لإقامة صداقات، وعزمي على معاملتها كمنتدى عام على غرار تويتر. وفتحتُ نِبذتي تماماً؛ بدأتُ بتلقّي كل طلبات الأصدقاء، حتى تلك التي تبعث على القشعريرة، ونظّفتُ نِبذتي من أية تفاصيل شخصية. (وافق فيسبوك في وقت لاحق على تسويةٍ تتعلق بالتُّهَم الموجَّهة من قِبَل لجنة التجارة الفيدرالية، والتي تزعم بأن تصرفات فيسبوك جائرة ومضلِّلة. ولكن تلك التسوية تمّت بعد عامَين من ترسيخ التغييرات - فات الأوان على إحداث أي فَرق).

كان الاسم التقني لطريقة عملي مع فيسبوك "خصوصية من خلال الغموض". فبدمج بيانات صالحة (علاقاتي الفعلية) مع بيانات سيّئة (الأشخاص الذين لا أعرفهم)، أمِلتُ في ألا تكون علاقاتي الحقيقية على مرأى من الجميع وسط العلاقات الزائفة.

ولكنني وجدت نفسي أُعقّم كل منشوراتي أثناء محاولتي مخاطبة جمهور متنوّع يتضمّن رب عملي، مصادري، أهل أصدقاء صغيرَيّ، وغرباء صادقتُهم في رحلة إلى البرازيل. لقد وجدت أن ما لديّ لقوله لهذا الجمهور المتنوّع يتناقص أكثر فأكثر. وفي العام 2012، تلاشت تحديثاتي إلى الصفر بالتحديد، وأدركت أن مقاربتي محت قدرتي على إقامة علاقة حقيقية مع أي شخص على فيسبوك.

مع ذلك، لم أكن مستعدة للتخلي عن فيسبوك تماماً. كنت ما أزال أريد التمكن من العثور على أشخاص وأن يعثر عليّ آخرون.

لقد فكرتُ مليّاً في ترتيب قائمة أصدقائي لتغدو صغيرة مِطواعة تحتوي على أصدقائي المقرَّبين، ولكنني أدركت أنني لا أُجاري في الواقع أصدقائي المقرَّبين والعائلة على فيسبوك (نستخدم البريد الإلكتروني، الرسائل النصّية، والهاتف). وعندما فكرت مليّاً في الاحتفاظ بقائمة أوسع من المعارف، وقعتُ في شرك قيام فيسبوك بتعريض قائمة أصدقائي للإفشاء بشكل متواصل.

وبحثت جيداً في إعدادات فيسبوك عن الخصوصية ووجدت أنها ما تزال لا تسمح لكم بحماية قائمة أصدقائكم تماماً. يقول فيسبوك: "يمكن للأشخاص على فيسبوك رؤية أصدقاء متبادَلين حتى ولو لم يكن بإمكانهم

رؤية قائمة أصدقائكم بالكامل".

بالنسبة إلى صحافية، إن ذلك القدْر من الإفشاء كبير. تخيّلوا موظفاً منخفض المستوى في مؤسسة يتودّد إلى صحافيّ ليشاطره المعلومات. فإذا لاحظ ناطق بلسان تلك المؤسسة نفسه أنه، أو أنها، يتشاطر، أو تتشاطر، "صديقاً متبادَلاً" مع صحافيّ، يمكن لهذا الإفشاء أن يجعل من الموظَّف مصدراً. يتعارض هذا الأمر مع تخفيض قائمة أصدقائي لتشمل الأشخاص الذين تربطني بهم علاقة في الواقع.

وفكرت مليّاً بمحو نِبذتي فقط. ولكنني ترددت ثانيةً بشكل غير منطقي في الإغلاق على آرائي.

كنت سأفتقد ثلاثة أمور في فيسبوك: (1) أحببتُ تمكّني من توجيه رسائل خاصة للناس عبر فيسبوك عندما لا تكون آخر معلومات الاتصال بهم متوافرة لي؛ (2) أحببتُ قيام فيسبوك بإبلاغي عندما يكون معرَّفاً بـي في صورة أو في موقع الآراء المنشورة (كي أطلب إزالة المعلومات المتعلقة بـي)؛ و(3) كوني صحافية وكاتبة، أحب أن "يعثر" عليّ الناس الذين يريدون قراءة كتاباتي.

لذلك، قررت الكفّ عن مصادقة كل أصدقائي عبر فيسبوك - أكثر من ستمئة - والإبقاء على نِبذة موجَزة لأجل توجيه الرسائل، وإزالة المعلومات التعريفية، وعثور أشخاص عليّ ربما يكونون راغبين في ذلك.

وثَبُتت صعوبة الكف عن المصادقة. لقد شعرت بالرهبة عندما حاولتُ الكف عن مصادقة طالب سابق في حساب التفاضل والتكامل، أو صفحةِ اجتماعيَ القادم مع زملاء الدراسة في المدرسة الثانوية.

انتهى بـي الأمر طالبةً من باحثتي السابقة، كورتني شلي، النَّقر على زر "أَلغِ الصداقة" لأجلي.

لقد تطلّبها الأمر سبع ساعات. ولكن بعد انتهاء الأمر، شعرتُ بحِمْل ضخم يُرفع عن كاهلي.

á á á

سرعان ما عثرتُ على جانب غير متوقَّع من العيش بدون فيسبوك: لم يَعُد الناس يتوقعون مني أن أعرف ما يحدث في حياتهم.

كنت في عشاء مع صديق لم أرَه منذ عشر سنوات تقريباً. وشرع بالتحدث عن إجازته في إيطاليا كما لو أنني أعرف التفاصيل، ومن ثم توقف."أوه، أجل، أنت غير مشاركة في فيسبوك"، قال. وأعاد سرد قصته منذ البداية (بالمناسبة، بدأتْ بولادة طفله - أمر أغفلتُه أيضاً).

لقد شعرتُ بارتياح كبير بسبب وجود عُذر لي لعدم متابعة مستجدات الناس عبر فيسبوك. عندما انضممت إلى فيسبوك في بادئ الأمر، وجدت أن دفق المستجدات يوفر شعوراً مواسياً بالأُلفة التي تربطني بأصدقائي البعيدين. ولكن عندما تعمّقتُ في البحث، أدركت أنه يمكن لهذا الشعور بالأُلفة أن يكون مضلِّلاً.

تعلّمتُ ذلك الدرس بالطريقة الصعبة عندما كنت في رحلة عمل إلى شيكاغو عام 2009 حيث التقيت أحد معارفي من الكلّية.

لم يسبق لي أن رأيته منذ سبعة عشر عاماً، ولكنني كنت أتابع مستجدات حياته عبر حسابَيه على فيسبوك وتويتر. لقد عرفتُ أنه فقد عمله مؤخراً وانتقل إلى شقة جديدة. حتى إنني عرفت ما واجهه من صعوبات لتثبيت دي أس أل في شقته الجديدة. لذلك، لم أسأله عندما التقينا شخصياً، "كيف حالك؟" بل اعتمدتُ مستوى من الأُلفة وسألت، "إذاً، كيف تجري أمور بحثك عن عمل؟"

لقد أجرينا حديثاً ممتعاً، ولكن بعد افتراقنا شعرت أنني نسيت أمراً ما. فاتصلت به وطرحت عليه السؤال الذي لم أطرحه: "كيف حالك، في الواقع؟"

لقد ثَبُت أنه يمر بوقت عصيب أكثر مما تصوّرت. كان وسط شراء شقة في مجمَّع سكني عندما فقد عمله، مما تسبب بفقدان قَرضه. لقد التزم بمغادرة شقته، لذلك تعيّن عليه التحرك بسرعة للعثور على مكان يعيش فيه. واعترف بأن المستجدات المنشورة عبر فيسبوك وتويتر عن وضعه "غير دقيقة" وأنه لم يشأ إثقال كاهل الناس بكثير من المعلومات.

شعرت بالغباء والسذاجة لأنني اكتفيت بحديث رقمي صغير وبشعور بالرِّضى عما قيل لي دون الذهاب بعيداً في بحثي عن واقع الأمور. وتعهّدت مذاك الحين فصاعداً بطرح السؤال التالي على الأشخاص الذين كوّنت معهم صداقات عبر الإنترنت، "كيف حالك، في الواقع؟"

أما الآن، وبعد فقداني كل أصدقائي على فيسبوك، انخفض احتمال استسلامي للأُلفة الزائفة التي توفرها مواقع التواصل الاجتماعي.

á á á

كانت إزالة معلوماتي عن وسطاء البيانات التجارية نوعاً مختلفاً من ممارسة الثقة: نوع الثقة التي تُولونها لمفتعِل غوغاء. أنتم تسلّمون الرشوة، ولكنكم لا تكونون واثقين تماماً من الحصول على نتيجة.

فالعديد من وسطاء البيانات يطلبون مني تقديم معلومات حساسة،

مثل رخصة السَّوق أو رقم الضمان الاجتماعي، لإتمام خيار عدم اشتراكي. حتى إن أحد المواقع طلب مني رقم بطاقة ائتمان. لذلك، تعيّن عليّ في كل حالة إجراء عملية حسابية: هل أثق بأن هذا الموقع لا يسيء استعمال معلوماتي؟ أم أن ترك بياناتي بين أيديهم وعدم تزويدهم بمعلومات إضافية يوفر لي مزيداً من الأمن؟

كنت قد ابتكرت قائمة من 212 وسيط بيانات أثناء تدقيقي، وسمح 92 منهم فقط بإتمام خياري بعدم الاشتراك. لقد طلب موقعان رسماً - طلب Mugshots.com 399 دولاراً لإزالة قائمة، وقال SearchBug.com إن تكلفة إزالة قائمة من "سجلاته الاستثنائية" المُعَدّة انطلاقاً من سجلات عامة عبر الإنترنت تبلغ 27,95 دولاراً. فقررت إغفالهما.

لقد طلبتِ الغالبية الساحقة مما تبقّى منها، خمسة وستون موقعاً، توفير معلومات شخصية من نوع ما بهدف إتمام خيار عدم اشتراكي. وطلب خمسة وثلاثون موقعاً تقديمَ بطاقة هوية من نوع ما، أو رقم الضمان الاجتماعي، أو بطاقة ائتمان، كي تتم العملية، في حين طلبت عشرة مواقع توفير رقم هاتف، وطلب أربعة وعشرون موقعاً إرسال عنوان منـزلي، وطلب أربعة وعشرون موقعاً إرسال استمارات إتمام خيار عدم اشتراكي بالبريد أو الفاكس.

مغمورةً بضخامة المهمة، قررت العودة إلى مبدأي التوجيهي المتمثل بـ"الدفع لقاء الأداء". سأشتري بعض المساعدة.

بالنسبة إلى وسطاء البيانات الكبار الذين يبيعون معلومات لمواقع البحث عن أشخاص عبر الإنترنت، ولسواها، لجأتُ إلى تراستد آي دي كاتالوغ تشويس (TrustedID Catalog Choice) - وهي شركة استهلّت عملها بمكافحة البريد التلقائي. فلقاء 35 دولاراً، وعدت الشركة بإتمام خيار عدم اشتراكي في وسطاء البيانات الأميركيين التسعة الأكبر حجماً، مثل أكسيوم وإكسبيريان.

وبالنسبة إلى مواقع البحث عن معلومات، تسجّلتُ لقاء مبلغ 209 دولارات لمدة شهرَين، في خدمة تدعى DeleteMe ، من إيْبين، وهي شركة في بوسطن في المرحلة الأولى من عملياتها المتعلقة بالخصوصية وقد ابتكرت أرقام الهاتف المخفية، وحسابات البريد إلكتروني، وبطاقات الائتمان التي استخدمتُها. قالت DeleteMe إنها ستُتم خيار عدم اشتراكي في المواقع السبعة عشر الأكبر حجماً، مثل إنتليوس وسبوكيو.

بعد أسابيع قليلة، بدا أن بياناتي تلاشت في الغالب من مواقع البحث

عن معلومات. وعندما بحثتُ عن اسمي على سبوكيو، وجدتُ أن النتائج الوحيدة كانت في آيداهو، وايومينغ، ويوتاه - ثلاث ولايات لم أعِش فيها أبداً. على WhitePages.com ، لم تكن هناك أية نتائج عن جوليا أنغوين.

ولكن بعد شهرين، كانت بياناتي ما تزال تظهر على أكبر موقع بحث عن معلومات - إنتليوس، يو أس سيرتش (Search US)، وزابا سيرتش (ZabaSearch). فاتصلت بجيم آدلر، الرئيس التنفيذي لشؤون الخصوصية في إنتليوس، أحد المدراء التنفيذيين القلائل لدى وسطاء البيانات الذين حضروا مؤتمرات عن الخصوصية وتلقوا اتصالات من مؤيّدين للخصوصية. (مذاك الحين، غادر إنتليوس للانضمام إلى شركة في المرحلة الأولى من عملياتها تملك مقداراً كبيراً من البيانات).

لقد أجرى بحثاً واكتشف أن إنتليوس لم تتلقَّ طلباً من إيْبين لإتمام خيار عدم اشتراكي. وعندما اتصلتُ بإيْبين، قيل لي إن تلكّؤ الشركة عن إحالة الأمر يعود إلى وجود "فيروس" في العملية.

مرتابةً، تحققتُ مجدداً مما إذا كانت الإتمامات الأخرى في إيْبين لخيار عدم اشتراكي قد أُنجزت. في الواقع، كانت ما تزال بياناتي تظهر على موقع آخر، هو يو أس أيه بيبل سيرتش (Search People USA)، قالت إيْبين إنها أتمّت خيار عدم اشتراكي به. وثَبُت أن هذا الموقع لا يقبل طلبات مماثلة من إيْبين أو من أي جانب آخر باستثناء الفرد المعنيّ نفسه.

اعتذرتْ محامية إيْبين، ساره دووني، وردّت مالي. ولكنها قالت إن وسطاء البيانات يتعمّدون تصعيب إتمام خيار عدم الاشتراك. "إنه أحد أسباب حثّي الدائم لإجراء إصلاحات تشريعية مرتبطة بمشكلة وسطاء البيانات: إنها مسألة قانونية، وقد يذهب مقدِّمو الخدمات المنكبّون على تلك المسألة بعيداً"، قالت. "نقوم بما أمكن، ولكن الأمر لا يكون كافياً على الدوام".

كان من الصعب التحقق من إتمام كاتالوغ تشويس خيار عدم اشتراكي. فوسطاء البيانات التجارية لا يعرضون البيانات التي يملكون. لذلك، اتصلتُ بكل منهم وسألت عما إذا كان اشتراكي قد أُزيل من قواعد بياناتهم.

جاءت النتائج صادمة للمشاعر. لقد أخفقت كاتالوغ تشويس في إتمام أكثر من نصف خيارات عدم اشتراكي التي وعدت بالقيام بها. وأخفقت في إحالة عمليات إلغاء اشتراكي إلى لكسيس نكسيس وداتالوجيكس. لقد أرسلت طلب إتمام خيار عدم اشتراكي لإبسيلون، ولكن العملية تمّت في قاعدة بيانات واحدة من قاعدتَي البيانات هناك. وأحالت عمليات إلغاء اشتراكي إلى

وسيطَي بيانات، آي - بيهافيور (I-Behavior) وكيه بـي أم غروب (Group KBM)، اللذَين قالا لي إنهما لا يقبلان طلبات من كاتالوغ تشويس لإتمام خيار عدم الاشتراك.

قالت ناطقة بلسان كاتالوغ تشويس إن المشاكل التي تعاني منها لكسيس نكسيس وداتالوجيكس مردّها "مسألة تكنولوجية" مرتبطة باليوم الذي عولِج فيه طلبـي. وعندما طلبتُ ردّ مالي، وافقت على ذلك.

لقد تعلّمتُ بمشقّة أنكم لا تستطيعون على الدوام شراء الخصوصية. فالخصوصية سِلعة قصيرة الأمد بصعب التحقق منها. لسوء الحظ، يسهل على الشركات استغلال ذلك الغموض لمنفعتها.

á á á

لم ينجح إنفاق المال على المشكلة، وكان ما يزال يتعيّن عليّ إتمام أكثر من خمسين عملية إلغاءٍ لاشتراكي.

فقررت إغفال المواقع المشبوهة التي تطلب معلومات شخصية لقاء إتمام خيار عدم اشتراكي. لم أشعر بالارتياح لوجوب إعطاء اسمي، وعنوان بريدي الإلكتروني، ورقم هاتفي المحمول لـ FreePhoneTracer.com لقاء إلغاء اشتراكي من موقعها الخدامتي الذي يوفر "إمكانية البحث عن معلومات معكوسة وتعقُّب أي رقم هاتف".

بشكل مماثل، قررت عدم إرسال رقم بطاقة ائتماني لـ MyLife.com الذي يوحي بحاجته إلى الرقم كي "أطالب بنِبذتي". وجاء في الموقع: "بعد التحقق من ملكية النِّبذة، سنحاول الامتثال لطلب الكتمان أو الإلغاء المقدَّم من قِبَلكم حالما يكون بالإمكان القيام بذلك بشكل منطقي".

ولكنني أرسلت للبقيّة رخصة سَوقي، بامتثال، وملأت الاستمارات عبر الإنترنت. لقد قضيت نحو ستين ساعة في تقديم طلبات لإلغاء اشتراكي وفي التحقق من إلغاء بياناتي. وقضت كورتني، باحثتي، ستين ساعة أخرى في جمع برامج جداول البيانات لأكثر من مئتَي وسيط بيانات.

ولكن موقعاً واحداً على الويب - PeopleSmart.com - أربكني. لقد اعتقدت أنني ألغيت بياناتي منه، ولكن كورتني قالت العكس. كنت في نيويورك وهي في اليابان حيث عملت أشهراً قليلة أثناء دراسة زوجها بموجب منحة دراسية.

لقد تبادلنا رسائل البريد الإلكتروني - وأدركنا أخيراً أننا نرى أموراً مختلفة على شاشتَي جهازَينا. في اليابان، رأت كورتني بياناتي على PeopleSmart . وفي نيويورك، بدت بياناتي مخفية. يبدو أن PeopleSmart

أخفت بياناتي عن نتائج البحث في الولايات المتحدة ولكنها أبقتها في نتائج البحث الدولي. "إنه أمر جدير بالازدراء!" قالت لي كورتني في رسالة بالبريد الإلكتروني.

يُعتبر هذا الأمر تصرّفاً ماكراً من قِبَل شركة تدّعي بأنها تعمل في ميدان "ابتكار الخصوصية". ففي مقطع من موقعها يدعى "كيف نحن مختلفون"، تقول PeopleSmart إن "إتمامها خيار عدم الاشتراك سهل ومجّاني" وهو الفارق الكبير بينها وبين مواقع أخرى للبحث عن معلومات تدّعي بأن "البعض لا يُزيل معلومات شخصية بالكامل، حتى بعد طلب ذلك".

لقد أوصلني قليل من التقصّي إلى الاستنتاج المفاجئ المتمثل بأن هذه الشركة هي في الواقع شركة في المرحلة الأولى من عملياتها في سيليكون فالي تدعى إنفليكشن. يصف موقعها على الويب الشركة بأنها "شركة في المرحلة الأولى من عملياتها مع مقدار كبير من البيانات" وتروّج لعلاوات يحصل عليها الموظفون مثل رحلات بحرية، تأمُّل، يوغا، ورياضات السير مسافات طويلة. فوجّهتُ لها رسالة غاضبة بالبريد الإلكتروني، مطالبةً بشرح.

حفاظاً على صِدقية الشركة، أجاب المدير التنفيذي الأعلى، ماثيو موناهان، على الفور تقريباً، واعداً بالنظر في الأمر. وبعد يوم، أرسل جواباً مفصَّلاً يشرح فيه قيام الشركة باستخدام مصادر بيانات مختلفة لأجل موقعها الدولي، وفشلتُ في إلغاء اشتراكي من مجموعة البيانات تلك. "لا وجود لسوء نيّة هنا"، قال لي عبر الهاتف بعد أسبوع. "لا نجني مالاً من المستخدمين الدوليين. حتى إنه ليست لدينا أية خيارات دولية لتقاضي المال. بالنسبة إلينا، كانت كوميديا أخطاء من نوع ما".

قال لي موناهان إنه وشقيقه الأصغر، براين، أسّسا إنفليكشن عام 2006 مع فكرة بسيطة عما ستغدو عليه. كَفّ ماثيو موناهان عن ارتياد جامعة كارولاينا الجنوبية بهدف إدارة شركة في المرحلة الأولى من عملياتها تبيع كتباً إلكترونية تتناول أفكاراً مفيدة عن كيفية دخول الكلّية. (هناك قرّاءُ كتب إلكترونية، لذلك وُضعت الكتب في ملفات بيي دي أف يمكن تحميلها). كان براين يدرس في هارفارد، وأفكارهما غامضة قليلاً: "قررنا الانتقال إلى كاليفورنيا، إلى مكان قريب من فيسبوك، ومواجهة صناعة غير فعالة"، قال لي ماثيو. وقررا أن يكون هدفهما الأول تحويل السجلات العامة إلى بيانات رقمية.

فأخذا المال الذي جمعه ماثيو من بيع مغامرته في الكتب الإلكترونية واستثمراه في صناعة تكنولوجيا تُحوّل سجلات المحاكم والسجلات العامة

للأشخاص إلى بيانات رقمية. لقد دُعي مُنتجهما الأول CallerID ، وهو يسمح لكم بإدخال رقم هاتف محمول والعثور على مالك الهاتف.

"لم نكن متطوّرين"، تذكّر ماثيو. وبعد قليل من إطلاق مؤسستهما، واجهت صناعة البحث عن معلومات حول الهواتف المحمولة ردة فعل شعبية معادية. ففي العام 2008، أطلقت إنتليوس خدمة بحث عن معلومات حول الهواتف المحمولة تسمح للناس بالبحث عن أرقام هاتف محمول من خلال اسم المستخدم. وادّعت إنتليوس تضمين الخدمة تسعين مليون رقم هاتف محمول. بعد أشهر قليلة، أغلقت إنتليوس الخدمة بضغط من فريزون ومؤيِّدين للخصوصية.

قرر الشقيقان التركيز على السجلات العامة التاريخية. ففي العام 2009، أطلقا GenealogyArchives.com ، التي أصبحت في ما بعد Archives.com ، لتوفير إمكانية ولوج سجلات تاريخية رقمية. في العام 2012، اشترت Ancestry.com موقع Archives.com بقيمة 100 مليون دولار.

بعد كسبهما غير المتوقَّع، كان بإمكان الشقيقَين التقاعد، ولكنهما قرّرا بدلاً من ذلك إعادة التركيز على خدمات البحث عن معلومات. فرمّما PeopleSmart.com ، وأطلقا موقعاً لدراسة التوظيف يدعى GoodHire.com ، وشرعا بالعمل على خدمة جديدة تدعى Identity.com تساعد الناس على إدارة معلوماتهم الشخصية عبر الويب. "أشعر فقط بأن عملنا غير مُنجَز"، قال ماثيو. "لا أشعر بأن لا شيء صائب باستثناء مواصلة العمل على المنتجات في الوقت الحاضر".

قال لي ماثيو إنهما حاولا جعل إتمام خيار عدم الاشتراك مهمةً سهلة بصفة خاصة بسبب وجودها على استمارة عبر الإنترنت، بخلاف ما هو الحال في مواقع أخرى ترغمك على إرسال رخصة سَوق أو طلب إلغاء اشتراك عبر البريد. "نعتقد أنها عملية شاقة بشكل متعمَّد"، قال لي ماثيو.

قال ماثيو إنه شعر بالخيبة عندما تلقّى بريدي الإلكتروني الذي يُفيد بأن إلغاء اشتراكي لم ينجح. قال في هذا الصدد: "قضينا كثيراً من الوقت لإنجاح هذا الأمر".

تتمثل المشكلة، برأيه، بخوارزميّة المطابَقة. لقد أخفقت أجهزتهم الكمبيوترية في مطابقة جوليا إنغوين التي ألغت اشتراكها في الولايات المتحدة مع جوليا أنغوين التي خُزِّنت سجلاتها في قاعدة بيانات ثانوية لأجل الاستخدام الدولي.

وبحسب رأيه أحد أسباب عدم نجاح الأمر: "لم نسألك عن رقم ضمانك الاجتماعي، لا نستخدم هذه الأرقام لمطابقة مجموعات البيانات. لذلك، علينا استخدام مجموعات أخرى". (قال لي موناهان في وقت لاحق إن الشركة حسّنت عملية إلغاء الاشتراك كي لا يحدث هذا الخطأ مجدداً).

قد لا يكون الأمر مقصوداً ولكنني لم أتمالك نفسي من التفكير في أن تقديم الخدمات بشكل جيد في سوق البيانات الشخصية يعود على المرء بالفائدة. فإذا ألغيتُ اشتراكاتي في كل قواعد البيانات المتوافرة، من شأن ذلك أن يجعل بياناتي أكثر نَدرة وقيمة بالنسبة إلى أولئك المتمسكين بها.

á á á

في النهاية، شعرت بأن خسارتي أكبر من كَسبي في عملية إلغاء اشتراكاتي. لقد اختبرتُ شعوراً بالخسارة عندما أقفلت حساباتي، وقلقتُ حيال إقفالي خيارات عمل مستقبلية محتمَلة، وتقليص "صحة معلوماتي" - قلّت إمكانية التحقق من صحة معلوماتي في اقتصاد البيانات الشخصية.

وبالرغم من كل تلك الخسارة، لم أنجح كلّياً في إلغاء اشتراكاتي. فبياناتي ما تزال مسجَّلة لدى أسوأ مقدِّمي الخدمات - أولئك الذين صعّبوا عليّ مهمة إلغاء اشتراكي. حتى إن أولئك الذين سمحوا لي بإلغاء اشتراكي لم يَعِدوا بمحو ملفاتي بل "بكتمانها" فقط.

من بين كل شبكات التعقُّب التي واجهتُ، كانت هذه الشبكة الأكثر تضليلاً في وعدها بتوفير خيار للمستخدمين في شأن بياناتهم.

الفصل الثاني عشر
قاعة المرايا

عندما شرعت راين بويرتوس بعمل جديد عند بائع أجهزة كمبيوتر بالمفرّق في تامبا، فلوريدا، لم تكن تحاول إخفاء مَيلها الجنسي، ولم تكن أيضاً تأمل في إحاطة زملائها الجدد عِلماً بالأمر. ولكن غطاءها أُزيل عندما تحققت من النِّبذة في حسابها على فيسبوك من خلال الكمبيوتر المشترك في غرفة الاستراحة. فانحنى أحد زملائها في اتجاهها وقال، "انظري - كل الإعلانات على صفحتك هي إعلانات لغير الأسوياء الجنسيين. ما سبب ذلك؟"

لقد هالها قيام إعلانات فيسبوك الموجَّهة بافتضاح أمرها.

قالت لي: "لقد افتُضح أمري، ولكن عندما أكون في العمل لا أكون هناك للتحدث عن حياتي الشخصية". بعد تلك الحادثة، بدأت تتحقق من نِبذتها على فيسبوك من خلال الهاتف وليس من خلال الجهاز المشترك في العمل.

لقد افتُضح أمر راين بواسطة إحدى أنواع شبكات التعقُّب البريئة كما هو مفترَض؛ قاعة المرايا التي يبتكرها المعلنون انطلاقاً من البيانات الشخصية التي يجرفونها عبر الإنترنت.

á á á

لقد أوجدت صناعة التعقُّب الإعلاني عبر الإنترنت إحدى شبكات التعقُّب الأكثر شمولاً في العالم.

فمعظم مواقع الويب تدعو عشرات شركات التعقُّب الإعلاني للتجسس على زائريها وتتبّعهم عبر الويب. في العام 2013، كانت هناك 328 شركة منفصلة تتعقّب زائرين على مواقع الويب الخمسين الأوائل، وفقاً لدراسة أجرتها كراكس ديدجيتال، وهي شركة تراقب تكنولوجيا التعقُّب الرقمي. إنه ضعف الشركات الـ167 تقريباً التي وجدت كراكس أنها تقتفي أثر زائرين على مواقع الويب الخمسين الأوائل عام 2011.

والمعلومات التي تجمعها شركات التعقُّب الإعلاني مفصَّلة تماماً. لقد صُدمت آشلي هيس - بيتي عندما علِمت بقيام شركة تعقُّب إعلاني بوضع ملف على جهازها يحتوي على رمز واحد - 4 c812db292272995e5416a323e79bd37 - يعرِّف عنها سرّاً بأنها أنثى في السادسة والعشرين من العمر في ناشفيل، تينيسي. علاوةً على ذلك، أعدّت

الشركة قائمة بأفلامها السينمائية المفضَّلة، بما فيها عروس الأمير ، أول *50* موعد ، و *10* أمور أكرهها فيك . "حسناً، أحب الاعتقاد بتبقّي بعض الغموض في شأني، ولكن الأمر ليس كذلك، كما يبدو!" قالت عندما أطلعتُها على ما تتضمن نِبذتها. "النِّبذة صحيحة بشكل مخيف".

لم تعرف كيت ريد، البالغة من العمر سبعة عشر عام، سبب رؤية إعلانات على الإنترنت عن فقدان الوزن فقط حتى أَرَتْها زميلتي في وول ستريت جورنال ، إميلي ستيل، أن شبكة ياهو! الإعلانية اعتبرتها أنثى بين الثالثة عشرة والثامنة عشرة من العمر ومهتمة بفقدان الوزن.

وعرّفت غوغل بشكل دقيق بما تحبه جينا معاس البالغة من العمر عشر سنوات من حيوانات أليفة، وصور فوتوغرافية، و"عوالم وهمية"، وما لذّ وطاب عبر الإنترنت كالرسوم المتحركة. "لا أحب أن يعرف الكل ما أفعل وأموراً أخرى عني"، قالت جينا لزميلي في وول ستريت جورنال ، ستيف ستكلوو، عندما أَراها ما تعرف غوغل عنها.

تفيد شركات التعقُّب عبر الإنترنت إن المعلومات التي تحصل عليها مجهولة الهوية، ولذلك فهي آمنة. إجابة نموذجية: قال ناطق بلسان غوغل إن تعقّب الموقع لجينا "قائم على نشاطٍ غُفْل على المتصفّح. لا نعرف ما إذا كان مستخدم واحد أو أربعة مستخدمين يستخدمون متصفّحاً محدَّداً، أو من هم أولئك المستخدمين".

ولكن هناك دليل متزايد على أن المعلومات المتوافرة عن العادات المتّبَعة عبر الويب لتتبُّع الأشخاص يمكنها التعريف بهم بشكل فريد. ففي العام 2006، نقّبت النيويورك تايمز في سجلات غُفْل للاستفهام عن أبحاث أطلقتها أيه أو أل، وتمكنت من معرفة الأبحاث التي أجرتها امرأة في الثانية والستين من العمر تدعى تيلما أرنولد. وفي العام 2008، نقّب باحثون من جامعة تكساس في سجلات غُفْل عن تأجير أفلام سينمائية أطلقتها نتفليكس، ووجدوا أن "باستطاعة منافس يعرف القليل فقط عن فرد ما أن يميّز بسهولة سجل هذا المنتسب في مجموعة البيانات".

علاوةً على ذلك، تتشاطر عدة مواقع على الويب، وبشكل غير متعمَّد، أسماء زائريها مع شركات التعقُّب الإعلاني. ففي العام 2012، سجّل فريقي في وول ستريت جورنال دخوله إلى سبعين موقعاً شعبياً على الويب تقريباً، ووجدوا أن المواقع تنقل لشركات طرف ثالث، في أكثر من ربع الوقت، الاسم الحقيقي للمستخدم، وعنوان بريده الإلكتروني، أو تفاصيل شخصية أخرى (مثل اسم المستخدم). حتى إن موقعاً رئيسياً للمواعدة أرسل المَيلَ

الجنسي لشخص يجاهر بهذا المَيل، وعاداتِه في تعاطي المخدرات، لشركات الإعلان.

ويمكن لكل أزرار "الإعجاب" على فيسبوك، وأدوات ربط "غرّد هذه القصة" على تويتر، معرفة المستخدمين بأسمائهم - حتى ولو لم يكن المستخدمون ينقرون على الأزرار. ففي العام 2012، وجد فريقي في وول ستريت جورنال أن 75 بالمئة من المواقع الألف الأولى على الويب تتضمن شيفرة من شبكات التواصل الاجتماعي يمكنها مطابقة أسماء الأشخاص مع عاداتهم بتصفّح الويب.

بالطبع، تقول الشركات أيضاً إن هذا التعقُّب المميِّز غُفل. "سنقدّم لك إعلانات بالاستناد إلى هويتك"، قال إرين إيغان، المدير التنفيذي لشؤون الخصوصية في فيسبوك، "ولكن ذلك لا يعني أن بالإمكان تحديد هويتك".

إنها رسالة قصيرة جداً. بالرغم من كل شيء، هل تُبالي راين حقاً بقيام فيسبوك "بتحديد هويتها" قبل افتضاح أمرها؟

á á á

ما تزال قاعة المرايا التي يبتكرها المعلنون بواسطة كل بيانات التعقُّب هذه غير مُتقَنة نوعاً ما. فغير الأسوياء الجنسيون يرون إعلانات لأمثالهم، والمهتمون بالنـزهات البحرية يرون إعلانات عن النـزهات البحرية. عندما كنت وزوجي نعيد تصميم منـزلنا، تسوّقتُ أحواض استحمام عبر الإنترنت وتبعتني إعلانات أحواض الاستحمام طوال شهر.

فكل شيء يبدو آمناً نوعاً ما، بالرغم من عمليات الافتضاح العرَضية.

لكن راين كالو، الأستاذ في جامعة واشنطن، يرسم صورة مُقلقة عن كيفية احتمال تطوّر قاعة المرايا. فهو يشير إلى دراسة أُجريت في جامعة ستانفورد أظهرت أن الفرد يستجيب بإيجابيةٍ أكبر لسياسيٍّ يدمج صورته ببراعة مع صورته أو صورتها. لا يمكن ملاحظة التغيير في الصورة، ولكنها تجعل الناظر أكثر تقبّلاً لرسالة السياسي.

"ثَبُت أننا نحب الأشخاص الذين يشبهوننا"، استنتج كالو. "الآن، تخيّلوا قيام شبكة تواصل اجتماعي بعرض خدمة مشابهة، تسمح للمعلنين بدمج الناطق بلسانهم مع صورة النِّبذة الخاصة بالمستخدم". لا عِلم لكالو بأي شخص يعتمد هذه التقنية. ولكنه يخمّن بأن هذا الأمر ليس بعيداً عن الوضع الحالي لإعلانات أحواض الاستحمام التي تتبعنا.

بالرغم من كل شيء، إذا كان باستطاعة مهندسي الطعام تصميم طعام تلقائي لاستهداف براعم مذاقنا، بصفة خاصة، وبطريقةٍ تجعلنا نستهلك المزيد،

وإذا كان باستطاعة شركات المقامرة صناعة آلات بيع ذاتي تشجّعنا على المقامرة أكثر فأكثر، لماذا لا يصمم المسوّقون إذاً حضورهم عبر الإنترنت للتلاعب بنا بطرق جديدة؟

كان فريق الخصوصية التابع لي قد كشف النقاب عن شركاتٍ تغيّر أسعارها استناداً إلى موقع المستخدم. لقد خمّن كالو أن الشركات ستجد قريباً طرقاً لتفصيل الأسعار بالاستناد إلى التاريخ الذي يكون فيه الناس أقل مناعة - ربما بعد يوم عمل طويل.

قد يتم التلاعب بالناس أيضاً لتقديم بيانات أكثر مما يرغبون في تقديمه، ويمكن للشركات استخدام تلك البيانات لاكتشاف المزيد عن كيفية استهداف ذلك الشخص. في إحدى الاختبارات، وجد باحثون في جامعة كارنجي ميلون أن بالإمكان التلاعب بالناس لتسليم مزيد من البيانات الشخصية على موقعِ تواصلٍ اجتماعي إذا مُنحوا "تحكماً ملموساً" أكبر ببياناتهم.

يقول كالو إن تلاعب السوق هو في الأساس "وَكْز لأجل الكَسب". ويستخدم المسوّقون، على الأرجح، كل الوسائل المتاحة لدفعنا برِفق في اتجاه منتجات أكثر كلفة أو للقيام بشراءات غير حكيمة. ويمكنهم القيام بذلك باستخدام المعلومات التي نتركها لهم للتحليل: إنه أثرنا البيانيّ عبر الإنترنت.

وهناك مكاسب حقيقية على المحك. لقد حلل بنيامين ريد شيلر، وهو أستاذ في عِلم الاقتصاد في جامعة برانديس، بيانات تتناول مجموعة واسعة من مستخدمي الكمبيوتر، ووجد أن باستطاعة نتفليكس رفع مكاسبها بنسبة 1,4 بالمئة إذا تبنّت أسعاراً مفصَّلة خاصة بكل فرد استناداً إلى السجلات التاريخية لتصفّح الزبائن الويب. وتبيّن له أن بيانات تصفّح الويب أكثر إنباءً من البيانات الديموغرافية المعيارية التي تتناول استعداد المستخدمين لدفع أسعار مرتفعة كي يتمكنوا من الاشتراك في نتفليكس. "يوحي هذا الأمر بأن تمييزاً في الأسعار من الدرجة الأولى قد يتطور من كونه تمييزاً نظرياً فحسب إلى تمييز عمليّ، ويُعتمد على نطاق واسع"، إستنتج.

á á á

أردت صدّ التعقُّب الإعلاني، ولكن تعيّن عليّ أولاً فرز كل المعلومات الخاطئة عن كيفية صدّ التعقُّب.

يعتقد كثير من الناس أن باستطاعتهم استخدام صيغة إينكونييتو (Incognito) في غوغل كروم، أو صيغة تصفّح خاص (InPrivate Browsing) في إنترنت إكسبلورر من مايكروسوفت لتجنّب التعرض للمراقبة

عبر الإنترنت. ولكن ذلك غير صحيح.

فصيغة إينكونييتو تحمي الخصوصية ضد تهديد واحد: الشخص الذي تتشاطرون معه جهاز الكمبيوتر. فبعد إنهاء جولة تصفّح الويب، تمسح الصيغة ببساطة بيانات التعقُّب الناجمة عن جولة التصفّح. ولكن مواقع الويب التي زرتموها عبر صيغة إينكونييتو تواصل تلقّي معلومات منكم - على غرار المتعقّبين على تلك المواقع.

لكن صيغة إينكونييتو بُنِيت لأجل أمر واحد: تصفُّح الأفلام والصور الإباحية. هي تُزيل بيانات التعقُّب التي تحمل أسماء إباحية، عن جهازكم كي لا يراها الشريك - الزوج أو الزوجة. ولكن موقع الويب والمعلنين على تلك المواقع يعرفون أنكم كنتم هناك.

لا أعتبر ذلك نموذجاً لرفع مستوى الأمن الكمبيوتري إلى الدرجة الفُضلى (Threat modeling). لذلك، كنت بحاجة إلى مزيد من التفحص.

كان توقفي التالي عند أداة اختيار عدم الاشتراك الخاصة بصناعة الإعلان. ولكنها تطلب مني تثبيت قَدْر قليل من البيانات (Cookies) المرسَلة من موقع على الويب والمخزَّنة في متصفّح المستخدم على جهازي لتنبيه شركات التعقّب إلى أنني لا أرغب في التعرّض للتعقّب. لقد بدا هذا الأمر أورويلياً على نحو غامض: تعيّن عليّ السماح لنفسي بالتعرض للتعقُّب كي لا أتعرّض للتعقُّب.

وحتى في هذه الحالة، تضمّنت قائمة الشركات المتعقّبة ستاً وتسعين شركة فقط، في حين أظهرت الدراسات الأخيرة وجود أكثر من ثلاثمئة شركة تعقُّب في السوق. تقول صناعة الإعلان إن الشركات المُدرَجة على قائمتها تشكل الغالبية العُظمى للتعقُّب الإعلاني، ولكنني أردت صدّاً شاملاً لكل الشركات التي تُعِدّ ملفات. لذلك، قررتُ إغفال اختيار عدم الاشتراك في صناعة الإعلان.

بعد ذلك، شغّلتُ زر "لا تتعقّب" على متصفّحي، وقد أرسل إشارة لشركات التعقُّب مفادها أنني لا أريد الخضوع للمراقبة. ولكن بما أن صناعة الإعلان لم توافق على الكفّ عن تعقُّب المستخدمين الذين يرسلون تلك الإشارة، كان تشغيل الزر احتجاجاً سياسياً ببساطة.

أخيراً، قررتُ التصرّف. ذات ليلة، وبعد خلود الصغيرَين للنوم، جلست إلى جهازي الكمبيوتري وحمّلتُ البرنامجَين الأكثر شعبية المضادَّين للتعقُّب على متصفّحي فايرفوكس.

لقد صدّ الأول، أدبلوك بلاس، عملية عرض الإعلانات - حارماً بذلك

المعلنين من فرصة إدخال بيانات متعقّبة إلى جهازي في المقام الأول. وبما أن مهنتي، الصحافة، تستمد الكثير من عائداتها من الإعلان، فإنني لا أؤيّد صدّ الإعلانات، ولكنني تصوّرت القيام بمحاولة باسم حماية نفسي من المراقبة.

وصدّ الثاني، نوسكريبت، شيفرة كومبيوترية من نوع ما تدعى جافاسكريبت (JavaScript)، إضافةً إلى برامج أخرى مثل فلاش، من تحميل صفحات ويب بدون إذني. يمكن استخدام جافاسكريبت لتحميل كل أنواع تكنولوجيا التعقُّب، بما فيها البيانات المرسَلة من موقع على الويب والمخزَّنة في متصفّح المستخدم؛ حتى إن بالإمكان استخدامها لمراقبة كيفية تحرّك فأرتكم على الصفحة. ولكن لديها أيضاً الكثير من الاستخدامات القانونية.

على الفور، توقف فايرفوكس فجأةً. عندما نقرتُ على صفحة أبل لإظهار نافذة جينيوس (Bar Genius)، لم يحدث شيئاً. لقد تعيّن عليّ اللجوء إلى استثناء على نوسكريبت (NoScript) لتشغيل جافاسكريبت من أبل.

حدث الأمر نفسه في Amazon.com . في بادئ الأمر، ظننتُ أن كل ما حاولتُ طلبه غير متوافر، ولكنني أدركت أنه يتعيّن عليّ اللجوء إلى استثناء أيضاً لأجل جافاسكريبت من أمازون.

في غضون يومَين، كنت مستعدة للتخلّي عنه. لقد تطلّبت كل صفحة زرتها مجموعةً ضخمة من القرارات في شأن الخطوط المسموح بها. لقد جلست ابنتي بجانبي وضحكتْ أثناء محاولتي تحميل صفحة وتصفُّح كل ما هو مُباح. وفوق كل شيء، كان أدلوك (Adlock) متعارضاً مع برنامج إدارة كلمة المرور، باسوورد1. ووجدت نفسي في النهاية مضطرة لإلغاء أدلوك بهدف التمكن من تشغيل باسوورد1.

ولكنني وجدت نفسي عالقةً مع نوسكريبت. وعندما أدركت طريقة عمله، بدأت أشعر بالغضب. لماذا يريد موقع البقالة على الإنترنت، فريشدايركت (FreshDirect)، تحميل خطوط من خمس شركات متفرّقة على جهازي الكمبيوتري أثناء قيامي بالتسوق؟ أنا أُنفق كثيراً من المال من خلال هذا الموقع، لذلك لا أتوقع منهم أن يوفروا ثقوباً للشركات التي تريد مراقبتي أتسوّق.

فالشركات التي يسمح لها فريشدايركت بمراقبتي هي:

- الشركة الإعلانية عبر الإنترنت التابعة لغوغل، دبل كليك (DoubleClick)؛

- أدذيس (AdThis)، وهي شركة تتباهى بتعقّبها 1,3 بليون مستخدم في الشهر؛
- كونفرج تراك (ConvergeTrack) التي تصف نفسها بأنها "إحدى التكنولوجيات الأكثر تقدماً في التعقّب والإبلاغ"؛
- بازارفويس (Bazaarvoice) التي تقول إنها "تصل مئات الملايين من المستهلكين ببعضهم البعض وبالأصناف التي يشترونها"؛ و
- كورومتريكس (Corometrics) من آي بـي أم التي توفر للزبائن القدرة على "توليد توصيات فورية في شأن المنتَج الذي يحمل طابعاً شخصياً بالاستناد إلى الاهتمامات التسويقية التاريخية والحالية للمستهلك".

إنها وصفة عن التلاعب المالي. أتخيّل عدم مرور وقت طويل قبل قيام آي بـي أم بتشغيل الأرقام ونُصح فريشدايركت بفرض أسعار أعلى عليّ عندما أتسوّق في وقت متأخر من الليل لأنني مرهَقة أو لأنني أبدو مستعدة للتساهل مع أسعار زبدة الفستق إذا كانت أعلى من أسعار اللحم البقري.

وسألتُ فريشدايركت عن العلاقات، ولكن الناطقة بلسان الشركة رفضت الإجابة عن أسئلتي. "مرحباً يا جوليا - لن نشارك في هذه القصة ولكننا معجَبون بما توصلتِ إليه"، أرسلتْ لي بريداً إلكترونياً بابتهاج زائف.

لم تحملني قراءة سياسة فريشدايركت حيال الخصوصية على الشعور بحال أفضل. لقد جاء فيها، "نتشاطر معلومات ديموغرافية مع شركائنا ومعلنينا على أساس غُفليّ وكلّي. هذا النوع من البيانات ليس مرتبطاً في الحال بأية معلومات يمكن تمييزها بطريقة شخصية". ولكنه قدّم لي خيار عدم الاشتراك بالبيانات التي يتم تشاطرها عبر البريد الإلكتروني، وهذا ما قمت به.

لقد أفقدني الاختبارُ عقلي. في الحياة الواقعية، لا تدعو سوبرماركت نصف دزينة من الشركات الأخرى إلى داخل المخزن لتشاهد الناس يتسوّقون. لماذا يُسمَح بذلك في العالم الرقمي؟

á á á

إذا كانت هناك أية مواساة، يشعر الشخص الذي ابتكر التعقُّب الإعلاني بالسوء حيال المدى الذي بلغه التعقُّب في عالم اليوم.

ففي العام 1995، كان دانيال جاي، وهو خرّيج من جامعة هارفارد، يبحث عن طريقة للمشاركة في الهوَس بالإنترنت. في ذلك الوقت، كان يدير قواعد بيانات فيدليتي التي يمكن للمستخدمين ولوجها من خلال تطبيق

خارجي (database Back-end)، وهي مهمة مُمِلّة بقدر أهميتها.

لقد أراد القيام بعمل أكثر إثارة للحماسة. لذلك انضمّ إلى الفريق المؤسِّس لشركة في المرحلة الأولى من عملياتها في بوسطن، تدعى إنغايج تكنولوجيز، تحاول نقل تكتيكات التسويق المباشَر إلى الإنترنت - من خلال تطوير "قوائم" بمشترين محتملين لمنتجاتٍ كالكتب الدراسية.

أما المشكلة التي واجهته: كيفية تمييز شارين محتملين؟ كان يرتاب في قيام الناس بملء استمارات عبر الإنترنت تشير إلى اهتماماتهم. "بسرعة كبيرة، بلغتُ الاستنتاج المتمثل بأن مصدر معلومات كبير سيثير اهتمام الناس كما تُثبِت سلوكياتهم التصفحية"، قال لي.

لذلك، شرع دان باستخدام ملفات نصّية صغيرة هي كناية عن بيانات مرسَلة من موقع على الويب ومخزَّنة في متصفّح المستخدم، بهدف تمييز أجهزة كمبيوتر الأشخاص الذين تصفّحوا موقعاً معيَّناً على الويب. في السابق، كانت هذه البيانات تُستخدم من قِبَل مواقع على الويب لتخزين بيانات حول تسجيل دخول المستخدم وكلمة مروره. كان يعتقد أن بالإمكان استخدام هذه البيانات أيضاً لتوليف معلومات عن عادات التصفّح لدى المستخدمين.

يكمن جمال هذه التقنية في غُفليّتها، ولا يمكن تحديد هوية مستخدمٍ للويب إلا من خلال رقمٍ يعرّف بالبيانات، وهي سلسلة طويلة من الأرقام المخصَّصة لجهازه الكمبيوتري. لقد ظنّ دان بأن طريقته حسّنت التسوّق التقليدي المباشَر حيث يشتري المعلنون ويبيعون قوائم بأسماء وعناوين أشخاص.

ولكن توقيت دان غير مناسب. فالإنترنت حديث العهد، والمعلنون القلائل الذين يشترون إعلانات غير قلقين على الاستهداف - سواءً كان غُفلاً أم لا. كان معظمُ مشتري الإعلانات عبر الإنترنت مواقعَ dot-com أخرى تحاول الترويج لعروضهم الأساسية العامة.

في غضون ذلك، كانت إنغايج تكنولوجيز وسط إعصار مواقع dot-com المقترب من اليابسة. فإنغايج جزء من تكتّل شركات إنترنت - تتراوح بين محركَي البحث ألتافيستا وليكوس، وموقعَي الويب Shopping.com و Furniture.com - نجمت عن فَورة بيع قام بها المقاول ديفيد ويذريل. وفي خريف العام 1999، ظهر ويذريل على غلاف بيزنيس ويك تحت العنوان الرئيسي "إنجيليّ الإنترنت". كان تجمّعه، سي أن جي آي، الطفلَ المدلَّل لازدهار مواقع dot-com ، مع مبادلات سوقية ضخمة بلغت 10

بلايين دولار، بالرغم من واقع تسجيل خسائر سنوية بقيمة 127 مليون دولار مقابل عائدات بقيمة 176 مليون دولار.

في العام 2001، انفجرت فُقاعة المبادلات السوقية عبر مواقع dot-com ، وبلغت خسائر سي أم جي آي بليون دولار في الربع الواحد من العام، وهوى سعر سهمها إلى أقل من دولار واحد. لقد غادر دان الشركة التي انهارت في نهاية المطاف. ولكن فكرة استخدام بيانات بهدف تعقُّب المستخدمين نجت.

في غضون ذلك، تصوّر دان أن تكون الخصوصية الأمر التالي الكبير. ففي العام 2001، أطلق شركة برامج للخصوصية تدعى برميسوس. لقد تمثلت فكرته ببيع تكنولوجيا للمؤسسات تساعدتهم في تعقُّب بيانات زبائنهم أثناء تنقّلها عبر أنظمتهم الكمبيوترية.

ولكن المؤسسات لم يكن لديها أي حافز لاتخاذ إجراءات صارمة حيال استخدامها الداخلي للبيانات. وبعد سنوات قليلة، انهارت الشركة وعاد دان إلى جذوره: الإعلان عبر الإنترنت. في العام 2007، كان ما يزال سوق الإنترنت يهمّ بالنهوض من إخفاق dot-com . فانضم إلى شركة في المرحلة الأولى من عملياتها تدعى تاكودا - البيانات المنسَّقة المستهدفة (TACODA-Targeted Data Coordinated) وتهدف إلى بناء النوع نفسه من النّبذات التي سعت إنغايج لابتكارها. "بدأنا بالتفكير في شأن استهداف السلوك - هذا الشخص يُنفق 30 بالمئة من وقته على الأخبار الدولية و20 بالمئة على الأجهزة الصغيرة و20 بالمئة على تذاكر كرة القدم"، قال لي دان.

للحصول على نظرة عامة عن سلوك الناس، كانت تاكودا بحاجة إلى تعقُّب شريحة واسعة من مواقع الويب. لذلك، شرعت تاكودا بالدفع لمواقع الويب التي توافق على وضع بياناتها الترصدية في أجهزة الكمبيوتر التابعة لزائري الموقع.

إنه تبدّل ضخم في السوق. في السابق، كانت مواقع الويب تتعقّب الزائرين لصالح معلنيها، ولا تبيع الآن بيانات زائريها لأحد بشكل أساسي. كان الأمر شعبياً بشكل مفرِط: تناضل مواقع الويب لبيع إعلانات، وتعرض تاكودا مالاً سخياً.

سرعان ما أصبح التعقُّب عبر الإنترنت المهنةَ الجديدة الرائجة. ففي العام 2007، باعت تاكودا ذاتها لـأيه أو أل بمبلغ 275 مليون دولار، ودفعت غوغل 3,1 بليون دولار لقاء دابل كليك، ودفعت مايكروسوفت 6 بليون دولار لقاء الشركة الإعلانية عبر الإنترنت، أيه كوانتيف.

ولكن التعقُّب الواسع النطاق ألحق الأذى بناشرين كباراً مثل وول ستريت جورنال و نيويورك تايمز . لم يَعُد المعلنون مضطرين لدفع رسم لبلوغ قرائهم على مواقع الويب؛ بدلاً من ذلك، يمكن للمعلنين تعقُّب أولئك القراء إلى موقع ويب آخر وشراء إعلانات أرخص على ذلك الموقع.

أصبحت البيانات التي تتناول القراء سِلعة. وحدها دُور المزاد العلني عبر الإنترنت، مثل بلوكاي، أصبحت مزادات علنية فورية للبيانات. كل يوم، تبيع بلوكاي ثمانية عشر قطعة من المعلومات تتناول عادات الأفراد في التصفُّح لقاء عُشر سِنت لكل قطعة.

يمكن للمزادات أن تحدث على الفور: عندما تَلِجون موقعاً على الويب، تباع صفاتكم في المزاد العلني للمزايد الذي يدفع المبلغ الأعلى. بعد ذلك، يعرض الفائز عليكم إعلاناً معدَّلاً وفقاً لطلب الزبون. ولكن دَفق البيانات حثّ بعض الشركات على استخدام تقنيات تعقُّب غازية.

بحلول العام 2010، شعر دان بالقلق من المعاني الضمنية لبيئة الغرب الجامح التي ساعد بنفسه على ظهورها. كان قلِقاً بصفة خاصة على المَيل المتزايد لمطابقة بيانات تتناول تصفُّح الويب مع الهويات الحقيقية للأشخاص ومع عادات التسوّق خارج الإنترنت. تجري المطابقة كالتالي: يسجّل المستخدم دخوله إلى موقع على الويب يتطلب إسماً، عنوان بريد إلكتروني، أو معلومة أخرى محدِّدة للهوية؛ تسحب شركة على ذلك الموقع، مثل أكسيوم، ملفّها عن الفرد وتخزّن بيانات مترصِّدة في جهاز المستخدم الذي يحتوي على بيانات الفرد ذاك - معلومات مسحوبة من سجلات الاقتراع، عنوان، دَخل، رَهن، ملكية مركبة آلية، وهكذا دواليك. تكون البيانات ما تزال غُفْلاً تقنياً، ولكن الكشف عن الهوية يكون وشيكاً. إذا كان المعلِن يعرف كل شيء عنكم باستثناء إسمكم، هل يهمّه الاسم حقاً؟

بسبب المطابقة عبر الإنترنت وخارجه، أُمطرت ليندا تومبلي، وهي في الستين من العمر وتُقيم في ناشوا، نيوهامبشير، بوابل إعلانات عبر الإنترنت عن المرشحين الجمهوريين أثناء انتخابات العام 2010. لقد اعتمدت شركة تدعى رابليف هذه التقنية للتعريف بنفسها بأنها محافِظة مهتمة بالسياسات الجمهورية، ومهتمة بالكتاب المقدس، ومساهِمة في القضايا السياسية والبيئة.

"دخان مقدَّس"، قالت ليندا بعد قيام زميلتي في وول ستريت جورنال ، إميلي ستيل، بفك شيفرة المعلومات في ملف رابليف الخاص بها. "الأمر أشبه بكلب حراسة يراقبني، وليس الأمر جيداً".

شعر دان بالقلق من قيام هذا التطور بتدمير الغُفلية التي حاول

بناءها بنفسه داخل النظام في الأساس. "عندما تمارسين مهنة رمي البيانات يميناً ويساراً، لا وسيلة للتحكم بها"، قال لي دان.

وفي العام 2011، أطلق شركة تدعى كورليت وأمِل في أن تعيد الخصوصية إلى عملية التعقُّب عبر الويب. يتمثل هدف كورليت بمساعدة الشركات على التثبّت من أن تترجَم إعلاناتهم على الويب مبيعاتٍ دون الإفشاء عن اسم الزبون وعن معلومات في شأنه. يستخدم فريقه في "غرف نظيفة" فعلية تقنيات متطورة في عِلم الرياضيات، محاولين إضفاء طابع الغُفلية على البيانات التي يستخدمون لمطابقة سلوك الزبائن عبر الإنترنت وخارجه. يتمثل الهدف بالسماح لتاجر سيارات هوندا بمعرفة أيٍّ من الإعلانات عبر الإنترنت يؤدّي إلى عملية شراء دون انتهاك غُفلية سلوك الفرد على الويب.

في ذِهن دان، إن التعقُّب المتغلغِل محتوم، ويتمثل هدفه بالحرص ببساطة على الإبقاء على غُفليّته.

á á á

بطرق ما، يخوض الناس المتقاتلين على بيانات التعقُّب الحربَ الأخيرة. وبما أن الناس أصبحوا واعين لتعقُّب هذه البيانات، شرع المسوّقون بالبحث عن تكنولوجيات تعقُّب جديدة. يُقال إن غوغل تطوّر شكلاً جديداً من التعقُّب غير المعتمد على البيانات المتوافرة يحدّد بطاقة تعريف فريدة لكل متصفّح على الويب.

ويتحرك مسوّقون آخرون في اتجاه تقنيات تحاكي "بصمة الإصبع - و ضع خارطة لملف كمبيوتري يتضمن مقداراً كبيراً من البيانات (computing Fingerprinting) - وتسمح لهم بتحديد جهاز المستخدم حتى ولو حاول صدّ التعقُّب من خلال برامج أخرى. "إذا كنت تريدين ألا يعرف أحد أي شيء عما تفعلينه عبر الإنترنت، لا تَلِجي الإنترنت"، قال المدير التنفيذي الأعلى لشركة تضع خارطة لملفات كمبيوترية تتضمن مقداراً كبيراً من البيانات.

والأكثر مدعاةً للقلق: إن بيانات التعقُّب التالية هي وجهك. فمع تحسّن تمييز الوجوه، يغدو من المحتمَل أكثر فأكثر ألا تكون قاعة المرايا ظاهرة على الويب فحسب. عندما تدخلون متجراً، يكون شركاء المبيعات على الأرجح قادرين على تحديد هويتك واستخراج البيانات نفسها التي تَلجها مواقع الويب حالياً.

تقدّم شركة تدعى فيس فيرست تكنولوجيا يمكن للباعة بالمفرّق

اعتمادها في متاجرهم لتصوير الزبائن وتمييزهم أثناء دخولهم الباب. "على الفور، عندما يخطو شخص ما موجود في قاعدة بياناتكم من فيس فيرست إلى داخل أحد متاجركم، يُوجَّه لكم تحذير من خلال بريد إلكتروني، نص، أو رسالة نصّية، تحتوي على صورته وعلى كل المعلومات البيولوجية المتعلقة بالفرد الذي تمّ التعرف إليه"، تقول الشركة في منشور إعلاني.

ووصف أحد مدراء البيع بالمفرّق لـ أل بيي ماغازين ، وهي مجلة تجاريّة تتناول صناعة منع سرقة وفقدان سِلع من مصادر متنوّعة، كيفية استخدام تكنولوجيا الغُفلية. قال مدير البيع بالمفرّق هذا، والذي مُنح الاسم المستعار "توم سميث، نائب رئيس منع سرقة وفقدان سِلع من مصادر متنوّعة في ستور - مارت"، إن سلسلة متاجر التجزئة، التي مُنحت الاسم المستعار "ستور - مارت"، تستخدمه لتمييز سارقي متاجر معروفين.

تعمل التكنولوجيا على هذا النحو: يُعتقل سارق متاجر في فرع لستور - مارت، وتُلتقط له صورة فوتوغرافية ويُطلب منه توقيع إنذار يوافق فيه على عدم العودة إلى المتجر. وإذا ظهر السارق مجدداً في ستور - مارت، تكون الكاميرات قد التقطت صورته وميّزته في غضون خمس ثوانٍ. ويُرسَل تنبيه إلى موظف في المتجر يدنو من السارق ويطلب منه مغادرة المتجر.

بالطبع، هناك مشكلة إجراءِ مطابقة خاطئة واستعداء أحد الزبائن. "إنه جزء مخيف بالنسبة إليّ"، قال سميث للمجلة، "التنبيه الخاطئ؛ الفتى الذي أطلق استغاثة كاذبة. ولكن التنبيهات الخاطئة منخفضة حتى الآن - نحو ستة تنبيهات من أصل مئة - لدرجة عدم بلوغ تلك المرحلة".

تتصوّر فيس فيرست مستقبلاً يتمكن فيه الباعة بالمفرّق من استخدام التكنولوجيا لأجل التسويق. ويقول المنشور التسويقي للشركة: "ابنوا قاعدة بيانات تحتوي على زبائن جيدين، ميّزوهم عندما يعبرون الباب، واجعلوهم يشعرون بأنه مرحَّب بهم أكثر فأكثر". وما لم يُفصح عنه هو كيفية معاملة الباعة بالمفرّق الزبائنَ الذين لا يحبونهم كثيراً، الأشخاص الذين يتسوّقون فقط عندما تكون الأسعار مخفَّضة، أو أولئك الذين يرتدون ملابس كثيرة على سبيل التجربة دون أن يشتروها.

أنا على ثقة تامة من أن قاعة المرايا القائمة على تمييز الوجوه لن تفيدني. فعندما يكتشف الباعة بالمفرّق أنني أم عاملة مستعجلة تفضّل الملاءمة على التوفير، أكون على الأرجح قد قررت شراء منتجات أكثر كلفة.

لم يكن هناك الكثير مما يمكنني القيام به. لقد حاولتُ إزالة معظم صوري عن الويب في مسعى لعدم المساهمة بأية قواعد بيانات لتمييز

الوجوه. ودفعتُ لفنان كي يرسم ستِنسل عن صورتي الفوتوغرافية، وبدأتُ باستخدامها على تويتر وفيسبوك. واستأجرتُ مصوّراً فوتوغرافياً كي يلتقط لي صورة أَمِلتُ في تمكني من استخدامها للترويج لمؤلَّفي ولكنها تحجب قسمات وجهي بما يكفي كي لا يكون بالإمكان استعمالها لتمييز الوجوه.

ولكنني قررت عدم ارتداء ملابس انسلالية: قَلنسوّة بيسبول مزوَّدة بمصابيح أل إي دي لإفشال عملية التقاط الصور، أو قَلنسوّة مضادة للطائرات بدون طيار تُحبط التصوير الحراري وقد ابتكرها أدام هارفي، مصمِّم حقيبة فاراداي لأجل هاتفي المحمول.

á á á

مع ذلك، واصلت خوض الحرب الأخيرة. فبعد شهر من استخدام نوسكريبت، أردت اختبار فعاليته. لذلك، اتصلت بأشكان سلطاني، الخبير التقنيّ الرائد في تكنولوجيا التعقُّب الإعلاني.

التقيت أشكان في بادئ الأمر، وكان قد تخرّج للتوّ من برنامج لنَيل الماجستير من كلّية المعلومات في جامعة كاليفورنيا. لقد أجرى هناك دراسة شاملة عن أنواع مختلفة من التعقُّب على الويب قام بها معلنون. بعد التخرّج، أقنعتُه بإجراء دراسة مماثلة لي لصالح جورنال ، وسرعان ما أصبح مستشاراً تقنياً في العديد من استقصاءاتنا الخاصة. مذاك الحين، قدّم أشكان شهادته مرتَين في الكونغرس عن الخصوصية عبر الإنترنت (مرتدياً بِذلته الوحيدة) وأصبح المصدر التقني الحاسم في شأن التعقُّب الإعلاني.

وافق أشكان على التحقق من فعالية تقنياتي في صدّ أعمال التعقُّب. وعملاً بتوجيهاته، غيّرت إعدادات قليلة في متصفّحي على الويب، وتدفّقت كل حركة اتصالاتي عبر الإنترنت إلى جهازه في العاصمة واشنطن.

"حسناً، أُدخلي موقع ويب"، قال. ونقرتُ على موقع الويب الخاص بمستخدِمي، WSJ.com

وشرع أشكان بقراءة أسماء شركات التعقُّب التي رآها في بياناتي. "تويتر، بلوكاي، دابل كليك"

"ماذا؟!" قلت. ظننتُ أنني صددت ولوجَها.

فشرح أشكان: كانت WSJ.com ترسل معلوماتي إلى بلوكاي، وهي شركة مزاد علني إعلانية عبر الإنترنت، فترسلها بدَورها إلى غوغل وياهو!. وبالرغم من صدّ نوسكريبت لجافاسكريبت، لم أتمكن من منع التنسيق بين شركات التعقُّب.

أما بالنسبة إلى تويتر، فقد نسيتُ قيامي بتسجيل دخولي إلى موقع

تويتر في وقت سابق، مما سمح له برؤية قيامي بزيارة WSJ.com .

تلك هي المشكلة مع التعقُّب على الويب: إذا سمحتم لشخص ما بدخول الخيمة مرة واحدة، يتمكن في غالب الأحيان من الحصول على ترخيص مرور مُباح لأعمال تعقُّب مستقبلية.

"هذا الأمر أسوأ بكثير مما ظننتُ"، قلت.

فضحك أشكان. "هذا ما قلتِه لي بالتحديد منذ ثلاث سنوات عندما أجرينا حديثاً للمرة الأولى".

وأراني أشكان الإعداد - مدفوناً عميقاً في قسم "تاريخ الزبون" في فايربوكس - الذي يسمح لي بمنع طرف ثالث، مثل تويتر، من تعقُّبي على مواقع أخرى لا لشيء إلا لأنني سجّلت دخولي إلى موقعهم. ولكن لم يكن هناك أي إعداد لصدّ مشاطرة جورنال وراء الكواليس.

لذلك، جرّبنا بعد ذلك أدلوك بلاس، ولكن بلوكاي كان ما يزال قادراً على عبور تلك المصافي. بالرغم من كل شيء، إن أدلوك بلاس مصمَّم لصدّ الإعلانات لا لصدّ التعقُّب. وبلوكاي ليس مُعلِناً بل مجرد شركة تغرف بيانات مستخدمين وتبيعها بالمزاد العلني. بشكل مماثل، تمكنت مجموعة من الشركات التحليلية، مثل أومنيتشر، من ولوج مواقعي. هي لا تبيع إعلانات بل تضع نِبذات عن المستخدمين.

إنها مشكلة رفع مستوى الأمن الكمبيوتري إلى الدرجة الفُضلى. لقد بُني أدلوك بلاس لأشخاص يعتبرون الإعلانات تهديداً، وبُني نوسكريبت لأشخاص يعتبرون تكنولوجيا معيَّنة - جافاسكريبت - تهديداً.

ولكن نظرتي إلى التهديد مختلفة: أردت صدّ التعقُّب سواءً كان مرتبطاً بإعلانات، أو بتكنولوجيا معيَّنة، أم لا. لذلك، حملني ذلك الأمر إلى نوع مختلف من تكنولوجيا الصد: شركات تضع قوائم متعقّبين.

جرّبتُ وأشكان عدداً قليلاً من الشركات التي تدير قوائم متعقِّبين. لقد تفاجأنا بالحصول على أفضل النتائج من شركة تصدّ المتعقّبين وتدعى غوستري (Ghostery).

طالما كنت مرتابة بغوستري منذ أن اشترتها شركة تلعب دوراً استشارياً في شؤون صناعة الإعلان. علاوةً على ذلك، تسمح غوستري بإجراء عمليات تعقُّب بشكل افتراضي. ولكن عندما عثرتُ على الإعداد الذي يوقف كل تعقُّب، أدركت أنه أكثر قوة من أي إعداد آخر.

راقب أشكان حركة اتصالاتي أثناء إبحاري من WSJ.com إلى Huffington-Post.com ومن ثم إلى Gawker.com . لم تظهر أية شركات

تحليلية، ولم تظهر بلوكاي. في الواقع، سرعان ما أدركتُ أن عدداً قليلاً من الإعلانات فقط ظهر. "إنه الأبرع الذي صادفتُه حتى الآن"، قال أشكان. "ولكن أي شيء لن يحميك تماماً".

á á á

لقد أثار غوستري اهتمامي. لماذا تُوفّر لي صناعة الإعلان أفضل طريقة لحماية نفسي منها؟

في العام 2009، أسس مقاول يدعى ديفيد كانسل غوستري (Ghostery) كبرنامج مجّاني إلى حد ما يُظهر للناس المتعقِّبين من كل جانب. وعام 2010، باعه لشركات خدمات إعلانية تدعى الآن إفيدن وعدتْ بالإبقاء على مجانية الخدمة، والمحافظة على خصوصية البيانات، وعدم استعمالها لغايات إعلانية. لقد وفت إفيدن بوعدها، ولكنها بدأت ببيع تحليل عن البيانات التي تجمعها غوستري لمواقعِ ويب ومعلِنين. حفاظاً على سمعتها، طلبت إفيدن من المستخدمين اختيار عدم الاشتراك في لوحة استخدام غوستري الغُفلية بدلاً من تشغيلها بشكل افتراضي. لقد انضم نحو ثمانية ملايين شخص. (أما أنا فلم أنضمّ).

قال لي أندي كال، مدير تحليل البيانات في إفيدن، إن مشتري البيانات هم في الغالب شركات تعقُّب تريد مراقبة منافسيها. في الواقع، بنت إفيدن دار مَقاصّة للمتعقِّبين كي يتعقّبوا أحدهم الآخر.

لقد استفدتُ من الاستخبارات التنافسية هذه. وعندما بدأت باستخدامها، كانت غوستري قد أعدّت إحدى القوائم الأكثر شمولية لتكنولوجيات التعقُّب المستخدَمة من قِبَل أكثر من ألف وستمئة شركة. وفي الشهر الأول من بدئي باستخدامها، أضافت غوستري مئة متعقّب جديد إلى القائمة.

ولكن انحياز غوستري المؤيّد للتعقُّب ألحق بـي الأذى. لقد أُعدّت غوستري للسماح بالتعقُّب بشكل افتراضي، مما يعني أنه تعيّن عليّ العبث بالإعدادات لصدّ أي تعقُّب. وبعد شهر من استخدام غوستري، لاحظتُ تواصل بعض التعقُّب. فشرح لي كال، قائلاً إن غوستري لا يصدّ تلقائياً متعقِّبين جدد أُضيفوا إلى القائمة. وأظهر لي الإعداد الذي سمح لي بإرغام غوستري على صدّ متعقِّبين جدد أيضاً. بدا الأمر ضرباً من ضروب التسلل بالنسبة إليّ، ولكن كال أكد لي أنها مجرد محاولة من غوستري لتسليمي زمام الأمور. "لدينا دافع للتحقق من قيامنا بالأمر الصحيح مع مستخدمينا لأننا لا نستطيع جمع البيانات التي تهتم بها الصناعة إلا إذا قمنا بعملنا"،

قال لي.

ولكنني كنت ما أزال أشعر بقليل من القلق حيال دوافع غوستري. هو يسيَّر لصالح صناعة التعقُّب وليس لصالح استخدام الناس له.

á á á

كان هناك برنامج يدعى ديسكونكت يصدّ التعقُّب بدوافع أفضل - أُسِّس من قِبَل منشقّ عن عالم التعقُّب.

بنى براين كينيش، وهو مهندس في غوغل، أول برنامج لصدّ التعقُّب بعد قراءة مقالة لزميلتي إميلي ستيل في وول ستريت جورنال عام 2010 فصّلت كيفية قيام فيسبوك بإرسال أسماء مستخدميها بشكل غير متعمَّد لشركات التعقُّب الإعلاني. لم يصدّق كينيش انتهاك فيسبوك الغُفليّة التي وعدت شركات التعقُّب على الويب بالمحافظة عليها. لقد عمل على الجانب الإعلاني لغوغل طوال ست سنوات تقريباً - وكان يعرف أن غوغل التزمت بالمحافظة على غُفلية بيانات التعقُّب على الويب.

في ذلك الوقت، لم يصدّ غوستري تعقُّب شبكات التواصل الاجتماعي مثل فيسبوك. لذلك، ذهب كينيش في ذلك المساء إلى منـزله ووضع برنامجاً صغيراً يدعى فيسبوك ديسكونكت (Disconnect Facebook) يمنع فيسبوك من تعقُّب المستخدمين عبر الويب. في غضون أسبوعَين، حظي برنامجه المجاني بقليل من الإعجاب في مجتمع التكنولوجيا وحُمِّل خمسين ألف مرة.

ولكن بغدوّ برنامجه أكثر شعبية، بدأ يفكر في التعقُّب الذي تقوم به غوغل. "إن تاريخ بحثك في غوغل، ياهو!، وبينغ، يعرّف بك بقدْر ما يعرّف بك تاريخك التصفّحي". قال لي كينيش. "أدركت أنه يتعيّن عليّ التخلّي عن غوغل للانكباب على ذلك".

لقد تخلّى عن غوغل في تشرين الثاني/نوفمبر 2010. وفي كانون الأول/ديسمبر، أطلق برنامجاً مجانياً يدعى ديسكونكت يمنع غوغل من جمع طلبات بحث عندما يسجل مستخدمٌ دخوله إلى بريد غوغل الإلكتروني أو خدمات أخرى لغوغل، ويمنع أيضاً تعقُّب شبكات تواصل اجتماعي مثل فيسبوك، تويتر، غوغل، ياهو!، وديغ.

أصبح ديسكونكت شعبياً على الفور، ولكن كينيش لم يكن واثقاً من أن ما يقوم به يُعتبر مهنة. فكل البرامج الأخرى المانعة للتعقُّب مجانية، لذلك لم يكن بإمكانه فرض رسم اشتراك. ولكن مواكبة كل تقنيات التعقُّب هو أشبه بسباق تسلّح، وكان بحاجة إلى موارد مالية لهذا السباق.

في بادئ الأمر، عمل في منـزله وعاش من مدّخراته. وفي تشرين

الأول/أكتوبر 2011، جمع 600,000 دولار من مستثمرين (بمن فيهم مؤسس غوستري، ديفيد كانسل) وتعاطى مع الأمر بجدّية.

ذهبتُ لزيارة كينيش في آب/أغسطس 2011. كان وفريقه المكوَّن من أربعة مهندسين محتشدين في قاعة اجتماعات صغيرة في سيليكون فالي، في مكاتب أحد داعميه الماليين، هايلاند كابيتال. كانت الظلال مُسدَلة والضوء الوحيد صادر من شاشات الكمبيوتر، وعلى الجدار شريط لاصق كان يثبّت سلةَ كرةِ سلة سقطت، ولديهم مجموعة من وجبات كوستو سريعة مكدَّسة فوق بعضها على طاولة. ولديهم أيضاً لوحة إحصائيات عن استخدام برنامجهم، وقالوا إنها دِعامة ضرورية في حال مرور داعم ماليّ ما لتطوير البرنامج.

لا يقود كينيش سيارة، لذلك أقلّيته بسيارتي المستأجَرة إلى المنـزل الذي استأجره مع عدد قليل من الزملاء. إنه المنـزل الأكثر قباحة في مجمَّعٍ سكنيّ جميل جداً. في الداخل، كان مرتَّباً ولكن مقتصِد ومزيَّن بطاولةٍ واحدة وأريكة.

"لديّ خمسة أشياء فقط"، حذّرني قبل فتح باب غرفة نومه. في الداخل فراش خفيف توأم. وفي الخزانة ثلاثة سراويل، وأربعة أحذية، وعدد قليل من القمصان مكدَّسة على الأرضية. فعدا عن جهازه الكمبيوتري، هذه الأشياء هي كل ما يملك.

"أعتقد أنه ربما يكون سبب عملي في ميدان البيانات"، قال لي. "لا أملك شيئاً. كل ما أملك هي البيانات".

أثناء تناول الغداء في بالو ألتو، أخبرت براين بأنني وجدت دوافعه مُربِكة. فالعيش كراهب هو أمر يلجأ إليه المقاولون عندما يراهنون على ثروة مستقبلية. ولكن هل يتوقع حقاً الاستفادة من السوق الهزيلة لبرامج حماية الخصوصية؟

قال إنه ما يزال يأمل في سوق الخصوصية. أولاً، قال، سينفصل المستخدمون عن المتعقِّبين. بعد ذلك، يمكن للمستخدمين الحصول على خدمة مدفوعة لإعادة وصلهم بشركات مختارة. أخيراً، قال، سيُجنى المال.

"أنا رأسمالي"، قال لي. "وأريد تغيير العالم".

أردت دعم مقاربة براين؛ فهي تتلاءم مع مبدأي التوجيهي المتمثل بالدفع لقاء الأداء. ولكن برنامجه التعقّبـي يصدّ شبكات التواصل الاجتماعي فقط، وأريد صدّ كل شيء. ففي حين كنت وأشكان نُجري اختباراتنا، كان غوستري يصدّ شبكات تواصل اجتماعي أيضاً، لذلك لم تكن هناك حاجة

لديسكونكت.

أخيراً، وفي نيسان/أبريل 2013، صدر برنامج كينيش. فقائمة المتعقبين التي يصدّ أطول من قائمة غوستري. إنه أشبه بسيارة صغيرة متينة. وعندما حاولتُ شراء بقالة عبر الإنترنت من فريش دايركت، صدّ ديسكونكت كل المتعقّبين، ولكنه منع أيضاً زر "الطلب" من الظهور على صفحة المغادَرة.

مع ذلك، تحوّلتُ لاستخدام ديسكونكت وقدّمتُ تبرّعاً من خلال رقم بطاقة اعتمادي المخفيّ الذي يمكن التخلص منه.

لقد اعتبرتُ أنني بحاجة إلى تمويل المتمرّدين في سباق التسلّح التعقُّبـي. بخلاف ذلك، وبدون وجود منافسة، من غير المحتمَل للخدمات الخيرية، مثل غوستري، التي توفرها صناعة التعقُّب، البقاء إلى جانبـي لمدة طويلة.

لقد ذكّرني الخيار بالأيام الأولى لحركة الطعام العُضوي. في غالب الأحيان، تكون أجنحة الغلال العُضوية في السوبرماركت مليئة بمنتجات متغضّنة ومبقَّعة. ولكن على مَرّ الوقت، وببطء، وبتزايد الناس الذين يشترون تفاحاً عُضوياً، تحسّنت النوعية. الآن، تكون الخُضار العُضوية جميلة المظهر في غالب الأحيان بقدْر جمال مظهر المنتجات التقليدية، لا بل أكثر جمالاً منها.

بالنسبة إليّ، كان استخدام ديسكونكت مماثلاً لشراء منتَج عُضويّ في الأيام الأولى. لقد اخترت دعم سوق برامج الخصوصية حتى ولو لم تكن منتجاتها برّاقة كمنتجات المنافسين.

الفصل الثالث عشر

شيفرات موحِشة

قبل ثلاثة أيام من حفلة عشاء عيد مولدي، أدركت أن أحداً لن يحضر إذا واصلت محاولة التواصل مع ضيوفي بواسطة الشيفرة.

فقبل شهر من الحفلة، أرسلتُ لكل من ضيوفي كتاب نيويورك السرّية: دليل غير عادي عبر البريد. وبعد أسبوع، أرسلتُ لهم عبر البريد "مفتاح شيفرة" يصف كيفية تحديد مكان كلمات وأحرف في الكتاب. على سبيل المثال (12،2،3،1) تعني الصفحة 12، السطر 2، الكلمة 3، الفصل 1.

بعد نفاد الوقت مني، أرسلت الدعوة النهائية، مكتوبة بشيفرة، عبر البريد الإلكتروني. جاء فيها:

(197،136) (377،23،7)

(23،4،10،1) (23،3،8،1) (29،27،4،1) (61،4،3)

(25،27،4) (25،27،3) (87،26،25)

(123،2) (393،1،2)

(113،14،14) (179،16،13) (159،41،4) (389،26،12) (95،30،11)

بعد فك الشيفرة، تقول الدعوة:

عشاء خاص

يوم 9/26

الساعة السادسة

المكان 41,5 الجادة الثانية

اشتروا تذكرة النَّفَق نقداً

وقبل أسبوع من الحفلة، بدأت أشعر بعصبية مزاج. لقد دعوت ستّاً من صديقاتي المقرَّبات، ولكن واحدة منهنّ فقط أبلغتني بأنها فكت شيفرة الدعوة. فارتبتُ في شأن قيام صديقاتي الأخريات بمحاولة فكّها.

حاولت التحقّق سرّاً من صديقة أخرى: "إذاً، ماذا ستفعلين في الأسبوع القادم؟" "أوه، سأقوم برحلة عمل"، قالت. لو كانت تعلم بأنها ستفوّت حفلتي لَذكرتْ ذلك. لقد أدركتُ حينذاك أنها لم تفك شيفرة الدعوة.

لسوء الحظ، إن الشيفرات غير ملائمة لتتزامن مع الروزنامة السابقة لحفلات العشاء في هذه الأيام.

أخيراً، اعترفت صديقة أخرى حائزة على دكتوراه في الفلسفة والطب

بأنها حاولت فك الشيفرة وأخفقت. "يا عزيزتي، أنا مولَعة بك تماماً... ولكنني غير مولَعة بفك الشيفرات"، كتبتْ. "لا أملك صبراً كافياً أو ذكاءً فطرياً للنجاح في امتحان حضور حفلتك!"

قبل ثلاثة أيام من الحفلة، أدركتُ أن أحداً لن يحضر باستثناء صديقة واحدة اتصلت لتُبلغني بأنها فكت شيفرة الرسالة. لذلك، ألغيتُ حجزي في المطعم - باسم آيدا، بالطبع - واتصلت بصديقتي لأُبلغها بأن الحفلة أُلغيت.

حلّ الموعد وولّى، ولم يذكر أيٌّ من ضيوفي الآخرين حفلةَ عشاء تحمي الخصوصية. بعد أسبوعَين، نظّمتُ حفلة عشاء أخرى، مستخدمةً بريداً إلكترونياً عادياً غير مشفَّر، وحقق الأمر نجاحاً تاماً.

ولكن العبرة من إقامة حفلة عشاء تحمي الخصوصية هي إخلاصي لاختباراتي المتعلقة بالشيفرة: غالباً ما يكون التواصل بالشيفرة عملاً موحِشاً.

á á á

لم أستطع تحميل صديقاتي مسؤولية إخفاق تحدّي التشفير.

كان "مفتاح الشيفرة" الذي أرسلته لهنّ صعباً لسببَين: (1) وصلت الدعوة منفصلة عن كتاب الشيفرات، مما تطلّبهنّ تتبّع الاثنَين؛ و(2) لم يكن استخدام كتاب الشيفرات لفك الشيفرة عادياً.

يُفترض بالتشفير الكمبيوتري الحديث حلّ المشكلتَين معاً.

اليوم، تقوم أجهزة الكمبيوتر بشكل سحري بالتشفير وفك الشيفرات. والأكثر إثارة للدهشة أنه لم يَعُد هناك كتب شيفرات. لديّ مفتاح شيفرة سرّي مخزَّن على جهازي الكمبيوتري لا يعرفه أحد سواي. ولديّ مفتاح شيفرة عام أنشره على موقعي على الويب لكل من يريد تحميله. معاً، يسمح لي ذانك المفتاحان بتشفير الرسائل وفك شيفرتها دون مراجعة كتاب شيفرات.

ولكنني أواجه وقتاً عصيباً في تجنيد أشخاص لتشفير البريد الإلكتروني. حتى إن العديد من أصدقائي المتسلّلين إلى الملفات الكمبيوترية رفضوا اعتماد التشفير معي - أعاد بعضهم السبب إلى عدم ثقتهم بقدرتي على التشفير بشكل صحيح، وقال البعض إنهم لا يثقون بقدرتهم على استخدام النظام البالغ التعقيد.

تأمّلوا بما تطلّبه الأمر لأُعِدّ نظام تشفير للبريد الإلكتروني.

أولاً، قمت بتحميل برنامج تشفير مجاني من جي أن يو برايفاسي غارد (GNU Privacy Guard) كي يساعدني على إدارة مفاتيح شيفرتي.

ولتوليد مفتاح شيفرة، يتعيّن عليّ تحريك فأرتي لمساعدة منتِج الأعداد العشوائية على تطوير مفتاح شيفرتي. عندما أحصل على مفتاح، أنقله إلى الجهاز الخادم الرئيسي العام ليتمكن الناس من البحث عني.

بعد ذلك، حمّلتُ برنامجاً يدعى إنيغميل (Enigmail) يُفترض به العمل مع بوستبوكس (Postbox)، وهو البرنامج الذي أستخدم لإدارة بريدي الإلكتروني. (جي بيي جي مصمَّم للعمل مع برنامج بريد إلكتروني تثبّتونه على جهازكم، وليس مع بريد إلكتروني تلجونه على الويب).

ولكنني لم أتمكن من حمل بوستبوكس وإنيغميل على العمل معاً. لقد طلبتْ صفحة دعم بوستبوكس الاتصال بإنيغميل لدى مصادفة أية مشكلة. وقالت منتديات دعم إنيغميل إن بوستبوكس ابتكر نسخته الخاصة عن إنيغميل غير المدعومة من قِبَل إنيغميل.

لقد وقعت في فخ فجوةٍ بين برنامجَين يُفترض بهما العمل معاً، ولكنهما لم يتعاونا، وشعرتُ برغبة في الغثيان. فنـزلتُ إلى الطابق السفلي، وسكبتُ لنفسي كأس خمر، وفكرتُ في سبب كفاحي لحل مشاكل تقنية. لا مشكلة لديّ في الكتابة وإعادة الكتابة، وهما أمران مماثلان. ولكن طالما جعلتني عملية حل المشاكل التقنية أشعر بالغثيان. أذكر قضائي ساعات في مختبر الكمبيوتر في الكلّية، محاوِلةً حل مشاكل برامجي - وشاعرةً بالغثيان نفسه وبالحاجة الملحّة نفسها للفرار.

لقد اعتبرتُ أن الرِّيبة هي المشكلة. أنا أقرأ كثيراً، لذلك أعرف معالم الكتابة. وعندما أراجع ما كتبتُ، غالباً ما أُحال إلى تكنولوجيات مستخدَمة من قِبَل كتّاب آخرين. ولكنني لا أعرف معالم حل المشاكل التقنية. نتيجةً لذلك، أشعر كما لو أنني أتعثر في الظلام دون أية نقاط مرجعية.

بالطبع، هناك كتيّبات تعليمات. لقد حمّلت بلهفة كتيّب كريبتوبارتي (CryptoParty) الذي يحتوي على صور إيضاحية مساعِدة لإعداد شيفرة للبريد الإلكتروني. ولكن التعليمات مخصَّصة لبرنامج البريد الإلكتروني ثاندربيرد (Thunderbird)، وليس لبرنامج بوستبوكس الذي أستخدم. في عالَم الأدوات التقنية المتغيّرة بسرعة، يصعب تحديث كتيّبات التعليمات باستمرار.

بعد كأس خمر وبعض التأمل، قوّيت عزيمتي وعدت إلى الطابق العُلوي للمحاولة ثانيةً. ولكنني كنت ما أزال غير قادرة على القيام بالأمر. وبعد جولة أخرى من المحاولات، استسلمتُ. أخيراً، أقنعت زميلةً أكثر ذكاء على الصعيد التقني بمساعدتي. في غضون ساعة، وجدتِ التعليمات (كان هناك بعضها) وحملتِ البرنامجَين على العمل معاً بشكل جيد.

كنت بحاجة الآن للعثور على بعض الأشخاص لتبادل بريد إلكتروني مشفَّر معهم. باستطاعتي العثور على كثير من الأشخاص المُدرَجين على الخادم الرئيسي لـجي بيي جي، ولكن من غير الواضح دائماً ما إذا كان الشخص المدرَج هو الشخص نفسه الذي أعرفه في الحياة.

على سبيل المثال، بعد المعلومات التي كشف عنها سنودن، وجدت ثلاثة مفاتيح شيفرة عامة خاصة بإدوارد سنودن مُدرَجة على الخادم الرئيسي العام لـجي بيي جي. فأحدها عنوان بريد لافابيت الإلكتروني، والآخر عنوان بريد بوز آلن الإلكتروني، والأخير عنوان البريد الإلكتروني ItAllGoesTo TheSamePlaceAnyway@anydomain.com . فمفتاح الشيفرة الأخير ليس سوى دُعابة، كما هو مفترَض. ولكن يمكن لأي شخص أن يَحزر المفتاحَين الأوّلَين الحقيقيَّين (عِلماً أنه ثَبُت استخدام سنودن عنوان لافابيت للوصول إلى العاملين الروس في ميدان حقوق الإنسان). لهذا السبب، هناك مناسبات يتحقق فيها أشخاص من الهويّات الرقمية لأحدهم الآخر ويوقّعون عليها (party Keysigning) قبل تحميل مفاتيحِ شيفرة ذاك الشخص.

ولكن التحقق من الهويات الرقمية بدا بالنسبة إليّ، وإلى حد كبير، مؤازَرة من قِبَل فيسبوك. تكمن الفكرة الرئيسية برمّتها في سرّية الكتابة المشفَّرة، إذاً لماذا أُعِدّ قائمة أخرى ظاهرة للعلَن بأشخاص تواصلتُ معهم وأُوليهم ثقتي التامة؟ بدلاً من ذلك، نشرتُ خارطة لمفتاح شيفرتي - سلسلة أحرف وأعداد من أربعين مكوِّناً - على موقعي على الويب لكل من يريد برهاناً على أنني المعنيّة.

عندما أعددتُ نظامي وسيّرته، وجدت متعة في تبادل رسائل بريد إلكتروني مشفَّرة مع عدد قليل من الزملاء والأصدقاء البارعين على الصعيد التقني. وظهرت رسائل في البريد الوارد بدت أشبه بكُتل طويلة وضخمة من الأعداد، والأحرف، والرموز، العشوائية. ولكن عندما أدخلتُ كلمة مروري، تحوّل النص العشوائي بشكل سِحري إلى بريد إلكتروني غير مشفَّر.

كنت أبدأ بالاستمتاع ببريدي الإلكتروني المشفَّر عندما صادفتُ الخبير التكنولوجي في أيه سي أل يو، كريستوفر سوغويان، في مؤتمر. كانت أولى إفشاءات سنودن قد ظهرت، وكنا نناقش الحاجة إلى بريد إلكتروني مشفَّر.

"أمقتُ حقاً استخدام جي بيي جي"، قال لي سوغويان. "من المعقَّد جداً أن تكون هناك فرصة جيدة كي يقوم أحدهم بالعبث عندما يستخدمه. أخشى من برود همّة المستخدمين إذا ما مُنحوا شعوراً زائفاً بالأمن، ومن كتابة أمر ما قد يُدخلهم في متاعب".

قال لي إنه يحتفظ بمفتاح شيفرته الرئيسي على قرص صلب مشفَّر في دُرج مُقفَل في مكتبه. هو يحتفظ بمفاتيح شيفرته الفرعية، التي تكون صالحة لمدة عام واحد، على بطاقة ذكية في محفظة جَيبه. ولقراءة أو كتابة بريد إلكتروني مشفَّر، يضع البطاقة الذكية داخل قارئ بطاقات ذكية موصول بجهازه الحضني، ومن ثم يُدخل كلمة مرور إضافية.

لقد شعرت بالإحباط على الفور. لم أكن أملك مفتاح شيفرة رئيسي أو مفتاحاً فرعياً، حتى إنني لم أكن أعرف أنني بحاجة إلى مفتاح رئيسي ومفتاح فرعي. لم يكن مفتاح شيفرتي في دُرج مقفَل أو على بطاقة ذكية، بل على جهازي الحضني.

في وقت لاحق، وفي مؤتمر إثر حفلة، أعربتُ عن أسفي لديفيد روبينسون، وهو مستشار قانوني وتكنولوجي ساعد على تأسيس مركز سياسة تكنولوجيا المعلومات في جامعة برينستون، بسبب عدم كفاءة برنامج جي بيي جي الذي أستخدم. وأراني روبينسون موقعَ ويب حملني على الشعور بأنني أفضل حالاً. إنه الموقع الشخصي لكارل فوغيل على الويب، وهو مطوِّر رائد للبرامج الكمبيوترية. عرض الموقع مفتاح شيفرته العلنية وشهادة التنصل هذه: "لا أثق بقدرتي على استخدام جي أن يو بيي جي (GnuPG)... يتطلب الاحتراسُ من [هجمات محتمَلة على جي بيي جي] حذراً متواصلاً، ولستُ على مستوى المهمة. لذلك، إذا وجدتم أهمية في أن تكون رسالتكم لي سرّية حقاً، رجاءً اتصلوا بـي قبل إرسالها، وسنعمل على معالجة المسألة".

á á á

يتمثل الخلل الكارثي في تشفير المفتاح العلني باعتماده على أفراد لحماية مفاتيحهم.

بالعودة إلى زمن كتب الشيفرة، كان جواسيس وعملاء عسكريون يتبادلون كتب شيفرة من خلال ناقلي رسائل مدرَّبين. ولكن علينا الآن إبقاء المفاتيح الخاصة مخزَّنة على أجهزتنا الكمبيوترية بفعاليةِ محافظةِ أولئك العملاء على كتب الشيفرة.

إنها مهمة مستحيلة في الأساس. فكمبيوتراتنا وهواتفنا الذكية عشوائية، وتجرف بيانات أثناء اتصالها بالإنترنت. ويمكن اعتراض كتب شيفراتنا عند الحدود حيث تستولي الحكومة بانتظام على أجهزة كمبيوترية وتنسخ كل محتوياتها بدون مذكرة تفتيش. في العام 2010، أطلق محقِّقو مركز التدقيق المُسبَق للهجرة والجمارك تحذيراً للسفر المستقبلي أعدّه ديفيد هاوس، وهو

مؤيّد لبرادلي مانينغ، الجندي الذي مرّر اتصالات الحكومة الأميركية لويكيليكس. وعندما عاد هاوس من رحلة إلى المكسيك، طُلب منه التوقف جانباً للاستجواب، وتم الاستيلاء على أجهزته. (قاضى هاوس وزارة الأمن الداخلي وتوصل أخيراً إلى تسوية قانونية وافقت الحكومة من خلالها على إتلاف البيانات التي حصلت عليها من أجهزته الإلكترونية).

كلما عرفتُ المزيد عن الأبحاث التي تُجرى على الحدود، ازداد قلقي من أن تكون بياناتي - صِلاتي، شيفراتي، وكلمات مروري - في خطر. لذلك، قررت البدء بعدم نقل أية بيانات عبر الحدود. ففي رحلة عمل إلى أوروبا، اصطحبت معي جهاز الكمبيوتر الحضني القديم الخاص بزوجي، ولم أصطحب أي هاتف. فلا ملفات أو بريد إلكتروني في الجهاز الحضني، وكنت أَلِج ملفاتي من مواردي المشفَّرة المتوافرة على سبايدرأوك وأسحب بريدي الإلكتروني من الويب.

ولكن مفاتح شيفراتي هي المشكلة. لقد أردت استخدام التشفير عندما أكون خارج البلد، لذلك وضعت مفتاح شيفرتي السرّي على قرص وامض، يو أس بـي، وخططتُ لإتلاف القرص قبل عودتي إلى الولايات المتحدة. ولكنني لم أخطط لكيفية إتلاف القرص، وعندما حان الوقت للمغادرة لم أجد الشجاعة للبدء بتمزيق القرص بواسطة مصباح في غرفة الفندق، بل محوت محتوياته وأَمِلت في حدوث الأفضل. لحسن الحظ، عندما وصلت إلى نيويورك، عبرتُ الجمارك بخفة وبدون أية مشاكل.

كان السفر بدون بيانات أمراً مريحاً على نحو مثير للدهشة. كنت أسجل دخولي إلى بريد إلكتروني كل مساء في الفندق، ولم أُغفل أي شيء. وكنت أكثر قدرة على التركيز على عملي بدون إلهاءٍ على الهاتف وأغنيةِ صفارة الإنذار التي يُطلقها باستمرار مع تواصل تلقّي اتصالات.

لقد اعتبرتُ أن عبور الحدود دون حمل أية بيانات ليس أمراً جيداً للخصوصية فحسب، بل لسلامة عقلي أيضاً.

á á á

لكن كتاب شيفراتي كان ما يزال عُرضة للخطر من قِبَل برامج ماكرة موجودة على جهازي الكمبيوتري - وهي في طليعة التجسس عبر الويب.

تأملوا بقصة حسين عبدالله، وهو مواطن أميركي ومدير أميركيون لأجل الديموقراطية وحقوق الإنسان في البحرين. ففي نيسان/أبريل 2012، كان يسير نحو الكابيتول هيل لإجراء لقاء تُناقَش فيه مسألة الإجراءات التي يتعرض لها المعارضون الموالون للديموقراطية في البحرين. أثناء سيره، نقر على

بريد إلكتروني مرسَل له عبر جهاز بلاك بيري من قِبَل صحافي، وجاء فيه "وجود حوار جديد - الوفاق وسلطة الحكومة"، مشيراً إلى الحزب السياسي، الوفاق، البحرينيّ المؤيّد لحركات الاحتجاج. حاول حسين تحميل الملف المُلحَق بالبريد الإلكتروني، ولكنه لم يعمل. مرتاباً، سلّم وناشطين بحرينيّن آخرين تلقّوا ملفات مُلحَقة مماثلة رسائلَ بريدهم الإلكتروني هذه لصحافيّ شجاع في بلومبرغ نيوز وضعها في عهدة باحثين في أمن الكمبيوتر لتحليلها.

بعد أشهر من التدقيق المُضني، وجد الباحثون أن الملفات المُلحَقة تحتوي على برنامج ماكر يمكنه، متى فُتح، تسجيل كل نقرات الناشطين على مفاتيح هواتفهم المحمولة، والتقاط صور للشاشة، وتشغيل الكاميرات والميكروفونات، والإصغاء إلى اتصالاتهم. كان البرنامج - الذي وضعته غاما غروب البريطانية - يرسل معلومات، كما يبدو، لأجهزة الكمبيوتر في البحرين. قالت غاما لبلومبرغ إنها لم تبِع البرنامج للبحرين، وربما سُرق برنامجها.

غاما رائدة في عالم التجسس عبر الإنترنت المتنامي بسرعة. تضع هذه الشركات برامج كمبيوترية تتحايل على التشفير، ويمكن لأدواتها تشغيل ميكروفون في جَيبكم والتقاط كل كلمة تقومون بإدخالها.

في تشرين الأول/أكتوبر 2011، ذهبتُ وزميلتي جنيفر فالنتينو- ديفريز إلى العاصمة واشنطن لزيارة آي أس أس وورلد، وهو مؤتمر تشتري فيه حكومات من مختلف أنحاء العالم أدوات تجسس عبر الإنترنت من شركات مثل غاما. ويُدعى أحياناً وايرتابرز بول.

من غير المفاجئ عدم تمكننا من الدخول، ولكن جنيفر تمكنت من الحصول على أكثر من مئتَي مستند تسويقي تعود لست وثلاثين شركة، بما فيها غاما. تروّج الكتيّبات لأدواتِ تسلّل إلى الملفات الكمبيوترية تمكّن الحكومات من اقتحام كمبيوترات الناس وهواتفهم المحمولة، واعتراض الأجهزة التي يمكنها جمع كل الاتصالات عبر الإنترنت التي جرت في بلد ما. لقد نشرنا الكثير من الكتابات عبر الإنترنت في قاعدة بيانات تدعى "كاتالوغ الرَّقابة: المكان الذي تحصل منه الحكومات على أدواتها".

يصف كتيّب فينسباي (FinSpy) من غاما غروب، وهو الأداة المستخدَمة لمراقبة الناشطين البحرينيّن، قدرةَ البرنامج على "مراقبة الاتصالات المشفَّرة". ويُفيد الكتيّب أيضاً بأنه استُخدم في مقهى للإنترنت بهدف مراقبة اتصالات سكايب (Skype)، لا بل التقاط صور الأشخاص أيضاً أثناء استخدامهم سكايب. "فينسبين حلٌّ للمراقبة البعيدة، أُثبتت فعاليته ميدانياً،

يمكّن الحكومات من مواجهة التحديات الحالية في ميدان مراقبة الأهداف المحمولة المُدرِكة للإجراءات الأمنية، والتي تغيّر موقعها بانتظام وتستخدم قنوات اتصال مشفَّرة وغُفْلاً، وتكمن في بلدان خارجية"، قال الكتيّب.

"راقبوا مئة ألف هدف"، هو العنوان الرئيسي لكتيّب شركة إيطالية تدعى هاكينغ تيم. "يمكن لنظام التحكم من بُعد مراقبة أهداف يصل عددها إلى مئات الآلاف".

قال لنا جيري لوكاس، منظِّم وايرتابرز بول، إن سوق الرَّقابة الفاعلة نَمَت من "الصفر تقريباً" قبل هجمات العام 2001 الإرهابية إلى نحو 5 بلايين دولار في العام.

"لا نتكبد عناء طرح السؤال التالي، هل هذا الأمر هو للمصلحة العامة؟" قال لوكاس.

á á á

أَمِلتُ في ألا أكون بحاجة للقلق في شأن قيام الحكومة الأميركية بتثبيت برنامج مراقَبة على جهازي الكمبيوتري أو هاتفي.

بالرغم من كل شيء، يبدو أن عملاء إنفاذ القانون في الولايات المتحدة حصلوا على مذكرة تفتيش لتثبيت برنامج مراقبة على كمبيوتر أو هاتف مشتبَه به. ففي حزيران/يونيو 2007، مثلاً، حصلت الأف بي آي على مذكرة تفتيش تسمح لها بإرسال برنامج جاسوسيّ إلى حساب على ماي سبيس لشخص يرسل تهديدات تفجيرية لمدرسة ثانوية قرب أولمبيا، واشنطن. (في قضية منفصلة، ردّ القاضي ستيفن سميث، وهو قاضٍ مساعد في تكساس رفض في الأساس إصدار أمرٍ لمراقبة موقعِ هاتف محمول، طلباً بالحصول على مذكرة تفتيش لتثبيت برنامج جاسوسيّ لأنه يعتقد، جزئياً، بأنه أقرب إلى رَقابة فيديوية منه إلى بحث تقليدي. على غرار التنصت على المكالمات الهاتفية، قد تتطلب الرَّقابة الفيديوية تبريراً إضافياً للمحكمة).

ولكنني قلقتُ حقاً على اتصالاتي المشفَّرة التي ينتهي بها الأمر في شبكات تعقُّب وكالة الأمن القومي. لقد ثبّتت الوكالة أجهزة تنصّت في شركات اتصالات محلية تملك القدرة على معالجة 75 بالمئة من حركة الاتصالات في الولايات المتحدة عبر الإنترنت، وفقاً لتقرير وضعه زميلاي سيوبان غورمان وجنيفر فالنتينو- ديفريز.

يُفترض بوكالة الأمن القومي إتلاف اتصالات محليّة بَحتة تعالجها عبر شبكات التعقُّب الخاصة بها. ولكن يبدو أن الوكالة وضعت استثناءً للاتصالات المشفَّرة. ففي مذكّرة كشف عنها إدوارد سنودن وتعود للعام

2009، قالت وكالة الأمن القومي إنها تحتفظ "بكل الاتصالات المشفَّرة أم تلك التي يُعتقَد لأسباب منطقية باحتوائها على معنى سرّي" - حتى ولو كانت اتصالات محلية بالكامل.

يعني ذلك أنني باستخدام التشفير أرفع على الأرجح راية حمراء تجرفني إلى داخل شبكة تعقُّب الوكالة.

لقد تمّ تحذيري في السابق. قال لي بيل بيني من وكالة الأمن القومي، حتى قبل ظهور إفشاءات سنودن، إن التشفير راية حمراء. "لا أثق بأي تشفير في الحقل العام. إذا لم يكن بإمكانهم اختراقه، يحصلون عليه من شبكة المعلومات"، قال لي. أضاف بيني أنه أرسل كل بريده الإلكتروني غير المشفَّر، عالِماً بأنه سيخضع للرَّقابة. "أُرسل كل ما هو بعيد عن الشك لأنني أريدهم أن يعرفوا كل شيء"، قال لي. "أَدعوهم غستابو ونازيّي البيت الأبيض".

ذات ليلة، التقيتُ كاشفي الأسرار الثلاثة في وكالة الأمن القومي، بيني، كيرك إيبـي، وتوماس دريك، حول مائدة العشاء في بيتيسدا. لقد نصحني إيبـي باستخدام أجهزة إرسال واستقبال راديوية جي أم آر أس (GMRS). واقترح بيني العودة إلى كتب الشيفرات الحالية الموزَّعة عبر البريد.

قال لي دريك إنه تعلّم درساً عندما كان مشرِفاً على متن طائرة مصمَّمة خصّيصاً لاعتراض اتصالات العدوّ. فأثناء تدريبات في نيفادا، تمكن فريقه من الإفلات من طائرة أف -15 مقاتلة من خلال مناوراتٍ مكّنتهم من التحكم برادارات دوبلر النَّبضية المعتمَدة في هذه الطائرة، سامحاً لهم بالتحليق على علوّ منخفض جداً والاندماج مع الانعكاسات التي تتسبب بها صفحة الأرض وتظهر على شاشة العرض.

"هكذا تُلحقين الهزيمة بالتكنولوجيا المتقدمة"، قال لي دريك، "بواسطة تكنولوجيا غير متقدمة".

á á á

كنت ما أزال راغبة في حل تكنولوجي، ويتمثل أحد الحلول المعتمَدة من قِبَل معظم أصدقائي المتسلّلين إلى الملفات الكمبيوترية ببروتوكول توجيهِ رسائل فورية مشفَّرة يُعرف بـتوجيه رسائل بشكل غير رسمي - Messaging Off-the-Record .

لقد ابتُكر البروتوكول عام 2004 من قِبَل نيكيتا بوريزوف وآيان غولدبرغ، تحت إشراف وإرشاد إريك بروير، وهو أستاذ علوم كمبيوتر في

جامعة كاليفورنيا في بركلي. إنه بروتوكول تشفير مجاني يمكن استخدامه بالإضافة إلى برامج توجيه رسائل فورية قائمة.

يساعد البروتوكول على حلّ مشكلة المستخدمين الذين هم بحاجة إلى حماية مفاتيحهم من خلال وضع مفاتيح جديدة فورية أثناء دردشات متكررة. يعني ذلك أنه يتعيّن على شخص يقوم بمراقبة الحديث وضع يده على المفاتيح أثناء الحديث.

نظرياً، يجعل هذا الأمر البروتوكول أكثر أماناً من البريد الإلكتروني المشفَّر، ولكن استخدامه لم يكن أكثر سهولة.

لاستخدام البروتوكول، تعيّن عليّ تحميل ثلاثة برامج كمبيوترية مختلفة وإقناعها للتعاون مع أحدها الآخر. أولاً، استخدمتُ برنامج الغُفلية الخاص بتور للاتصال بالإنترنت. بعد ذلك، اشتركت في حساب على جابر (Jaber) لتوجيه الرسائل الفورية. وحمّلت من ثم برنامجاً لتوجية الرسائل الفورية يدعى أديوم (Adium) ويحتوي على البروتوكول المذكور. أخيراً، أعددتُ أديوم للعمل مع تور وجابر.

يعود السبب الوحيد لتمكّني من القيام بأي من هذه الأمور إلى قيام الباحث في أمن الكمبيوتر، يعقوب أبلبوم، بمواكبتي في كل خطوة والقول لي أين أنقر وما أكتب في الإعدادات.

مع ذلك، كانت خَبيصة البرامج المجانية هذه أحدث ما توصّلت إليه الاتصالات المشفَّرة. ووجدت أن العديد من مصادري الصحافية الحساسة تريد مكالمتي فقط عن مزيج تور، جابر، وبروتوكول توجيه الرسائل. وللمصادر الأكثر حساسية، كنت أستخدم أحياناً، في الواقع، تور، جابر، وبروتوكول توجيه الرسائل، على جهاز كمبيوتر غير خاضع لأية رقابة أشغّله بواسطة قرص وامض يحتوي على نظام التشغيل تايلز (The Amnestic Incognito Live System-Tails). فتايلز برنامج مجاني شيفرةُ المصدر فيه متوافرة لعامة الناس، وهو سهل على نحو مفاجئ عندما يضعه لي صديقٌ متسلّل على قرص وامض. والأمر المثير للدهشة في تايلز أنه مصمَّم من الأساس لحماية الخصوصية، لذلك لا وجود لإعدادات أو لاختيار عدم الاشتراك. كان استخدام تايلز نظرتي السريعة الوحيدة والفُضلى إلى داخل عالَم متناوِب حيث يمكن إهمال الخصوصية.

أثناء دعواه القضائية في المحكمة العسكرية، وصف برادلي مانينغ، الجندي الذي مرّر اتصالات الحكومة الأميركية لويكيليكس، كيفية قيامه بالاتصال بويكيليكس من خلال تور وجابر لإجراء دردشاتٍ مشفَّرة. "سمحت

لي الغُفلية التي يوفّرها تور، ومعايير جابر، وسياسة منظمة ويكيليكس، بالشعور بإمكانية أن أكون ذاتي، متحرراً من قلق التصنيف الاجتماعي والأحاسيس التي غالباً ما تُنسَب إليّ في الحياة الحقيقية"، قال مانينغ في إفادته أمام المحكمة.

بالطبع، لم يُنقذ التشفير مانينغ في نهاية المطاف. لقد تعرّض لخيانة صديق - متسلّل إلى الملفات الكمبيوترية يدعى أدريان لامو، وقد سلّم مانينغ للأف بـي آي. عثر المحققون الحكوميون في وقت لاحق على أثار مراسلات مانينغ على جهازه الكمبيوتري؛ كان جوليان أسانج على "قائمة أصدقاء" مانينغ في جابر.

وهكذا، يمكن لهذه الهيكلية الصعبة المِراس المصمَّمة للكتمان الكشفَ عن الكثير. والخدمات الثلاثية العاملة معاً بارعة إلى حد كبير. ويمكن لأي تغيير في خدمة ما إحداث تغيير في الخدمتَين الأُخريَين. على سبيل المثال، بعد عام من إعدادي للخدمات الثلاثية، غيّر تور إعدادات وكيله، وتطلّبني الأمر أسابيع لاكتشاف سبب توقف جابر عن العمل.

لم أستطع إلقاء اللوم على مطوّري البرامج. فتور هو الوحيد بين البرامج الثلاثة الذي لا يتقاضى واضعوه أجراً. ويسيَّر جابر بواسطة متطوّعين يناضلون للدفاع عنه من هجمات التسلل المتكررة أثناء تسييره على أجهزة كمبيوتر ممنوحة. وبروتوكول توجيه رسائل بشكل غير رسمي هو مشروعُ متطوّعين بقيادة المؤسس أيان غولدبرغ، وهو الآن أستاذ في جامعة واترلو.

وأدميوم (Admium) مشروعٌ بقيادة إيفان شوينبرغ وتتوافر شيفرة المصدر فيه لعامة الناس. لم تكن هناك معلومات كثيرة عنه على موقع الويب، لذلك اتصلت به. لقد ثَبُت أنه طبيب عيون يُنهي عامه الرابع كطبيب مقيم. لقد استهل أدميوم في الكلّية، وحاول إبقاءه في حال جيدة. "ظننتُ عندما انتسبت إلى كلّية الطب أنني سأنتقل إلى مرحلة أخرى - سأسلّم زمام الأمور لشخص آخر"، قال لي شوينبرغ (كان لديه وقت للتحدث بسبب هدوء حركة العمل في المستشفى). "ولكن لم يكن هناك أبداً من يملك خبرة في البرمجة ويبدو راغباً في التورط بالقيادة". وهكذا، ذَبُل أدميوم. "لم أملك الوقت ببساطة، وانتقل عدد كبير من فريق التطوير الأساسي إلى أعمال تعود عليهم بالمال"، قال لي شوينبرغ.

على هذا الأساس الهش يكمن أملي الأكثر صلابة بالتشفير.

á á á

لم يكن يُفترض بالأمور أن تؤول إلى ما آلت إليه.

عندما أطلق الناشط المناهض لاستعمال الأسلحة النووية، فيليب زيمرمان، أول برنامجٍ تشفير لنطاق واسع من السوق يدعى بريتي غود برايفسي (Privacy Good Pretty) عام 1991، بدا الأمر كما لو أن وقتاً طويلاً لن يمرّ على تحرير الإنسانية من الظلم.

كان بيي جي بيي أول برنامج يوفر للناس العاديين إمكانية ولوج تشفير الرُّتَب العسكرية. حتى ذلك الوقت، كان التشفير القوي المعالَج على أجهزة الكمبيوتر متوافراً للحكومة فقط ولشركات كبيرة مستعدة لدفع رسوم ترخيص ضخمة. (البرنامج الذي كنت أستخدم للتشفير، جي بيي جي، هو نسخة مجانية عن بيي جي بيي).

لقد ساعد التوافر الواسع الانتشار للتشفير القوي على تحفيز حركة تدعى سايفربانكس - مجموعة مفكّرين ومبرمجين وباحثين مخصصة لحماية حرية الفرد في التعبير (Cypherpunks). ففي 9 أذار/مارس 1993، نشر إريك هيوز بيان مبادئ سايفربانك . "الخصوصية هي قوة الكشف عن الذات للعالم بشكل اختياري"، كتب هيوز. "عندما أشتري مجلة من متجر وأدفع نقداً للموظف، لا حاجة لمعرفة من أكون... عندما تُكشَف هويّتي من قِبَل آلية العملية التجارية الضمنية، لا أكون أتمتع بالخصوصية. لا يمكنني هنا الكشف عن نفسي بشكل اختياري؛ يجب عليّ الكشف عن نفسي دائماً ". لقد اتصل بالسايفربانكس لبناء أنظمة تسمح للناس بعدم الكشف عن هويّتهم. "علينا الدفاع عن خصوصيتنا إذا كنا نتوقع وجود أيٍّ من هذه الخصوصية"، كتب. "يدافع الناس عن خصوصيتهم منذ قرون بالهمسات، وتحت جُنح الظلام، وبالمغلفات، والأبواب المُغلَقة، والتصفحات السرّية، والمراسيل. لم تسمح تكنولوجيات الماضي بوجود خصوصية متينة، ولكن التكنولوجيات الإلكترونية تسمح بذلك".

من غير المفاجئ ألا تشعر الحكومة الأميركية بالإثارة بسبب انتفاضة السايفربانك. وشرع جهاز خدمة الزبائن الأميركي بالتحقق مما إذا كان زيمرمان قد انتهك قوانين تهريب الأسلحة بما أن التشفير ذات الطاقة العالية يُعتبر عِتاداً خاضعاً لقيود التصدير. ولكن الحكومة تخلّت عن التحقيقات في العام 1996 دون توجيه أية تُهَم. وفي العام 1999، أنهت الولايات المتحدة الحظر على تصدير منتجات تشفيرية.

حاولت وكالة الأمن القومي استيعاب الحركة بطريقة مختلفة. لقد طوّرت "رقاقة كليبر" لتشفير البثّ الصوتي، والقصد من ذلك: تخزين نسخات عن مفاتيح الشيفرات لدى الحكومة، مما يعني أن باستطاعة الحكومة فك

شيفرة كل شيء.

في العام 1994، كشف مات بليز في مختبرات أيه تي إند تي بِل عن خلل أساسي في رقاقة كليبر تغاضى عنه المؤيّدون - من الممكن إرسال مفتاح شيفرة خِدعة لا فائدة منه للحكومة ومواصلة استخدام التشفير. مُحرَجة، وضعت وكالة الأمن القومي المشروع جانباً بعد مدة قصيرة، مقدّمةً للسايفربانكس فوزاً مُبيناً. معتدّاً بنفسه بسبب الانتصار، كتب سايفربانك بارِز، هو بروس شنيير، في كتابه كتابة مشفَّرة تطبيقية العائد للعام 1996: "من غير الكافي حماية أنفسنا بالقوانين؛ نحن بحاجة لحماية أنفسنا بالرياضيات".

ولكن ثَبُت أن الكتابة المشفَّرة لا تستطيع الحماية من القانون. لقد بنى السايفربانكس مواقع على الإنترنت يرسَل إليها بريد إلكتروني كي يوجَّه إلى مقصده دون إخفاء عنوان البريد (Remailers) - خدمات تسمح للمستخدمين بتوجيه رسائل غُفْل مشفَّرة، وذلك عندما لم يكن من السهل ولوج حسابات بريد إلكتروني يمكن التخلص منها بسهولةِ ولوجها اليوم. ولكن في العام 1996، أغلقت الخدمة الأكبر، القائمة في فنلندا، بدلاً من الامتثال لأمر محكمة بالكشف عن هوية مستخدمٍ ما سبق له أن استعان بالخدمة لتوزيع معلومات تنتقد كنيسة المذهب الديني العِلمي.

لم تتمكن الكتابة المشفَّرة أيضاً من التغلب على تحديات كلمات المرور السيئة، وأجهزة الكمبيوتر غير الآمنة، والبرمجة الكمبيوترية غير المتقَنة.

بحلول العام 2000، أصدر بروس شنيير تعديلاً لحماسته السابقة. ففي كتابه أسرار وأكاذيب ، أعلن أنه كان مخطئاً في حمل القراء على الاعتقاد بأن "الكتابة المشفَّرة نوع من الغبار الأمني السحري يمكنهم نثره فوق برامجهم الكمبيوترية وجعلها آمنة". كتب شنيير أنه بات يعتقد بأن الكتابة المشفَّرة لم تكن المشكلة، بل الأشخاص الذين يستخدمونها. "الرياضيات منطقية؛ الناس ضالّون، مِزاجيون، وبالكاد يمكن فهمهم"، إستنتج.

طالما استغلت وكالة الأمن القومي مِزاجية البشر للتحايل على الكتابة المشفَّرة. ففي العام 2013، أوجزت مستندات كشف عنها إدوارد سنودن "الجهدَ العدائي المتعدد المظاهر الذي تبذله الوكالة لاختراق تكنولوجيات التشفير عبر الإنترنت" من خلال إقناع شركات التكنولوجيا بتمكين المستخدمين من لوج وكالة الأمن القومي لتتمكن من إضعاف معايير التشفير من خلال شن هجمات مستهدفة بواسطة برامج كميوترية.

وفي خضمّ الاحتجاجات الشعبية على هجمات الوكالة، قامت هذه

الأخيرة باستخدام تكتيكات متحايلة تشير ضمناً إلى عدم تمكنها بعد من حل رموز الصِّيَغ الرياضية التي تدعم الكتابة المشفَّرة الرئيسية العامة.

لقد أعلن شنيير، الذي راجع مستندات سنودن لصالح غارديان : "ثِقوا بالرياضيات. التشفير صديقكم. استخدموه بشكل جيد، وابذلوا قُصارى جهدكم لضمان عدم تعريضه للخرق. هكذا يمكنكم البقاء آمنين ولو في وجه وكالة الأمن القومي".

á á á

بطرق ما، تعود حركة سايفربانك إلى الحياة.

لقد حوّل جوليان أسانج، وهو عضو في سايفربانك منذ زمن بعيد، العلاقة بين الصحافيين ومصادرهم بعد إطلاق خدمة ويكيليكس المشفَّرة عام 2006، واعدةً الأشخاص الذين يريدون تسريب معلومات بغُفلية تامة.

وركّز سايفربانكس آخرون على وضع "تكنولوجيا تحرير" للمساعدة على تحرير الناس من الأنظمة القمعية. لقد وضع موكسي مارلينسبايك في سان فرانسيسكو تطبيقات تشفيرية - ريدفون (RedPhone) وتكست سيكيور (TextSecure) - لأجل هواتف أندرويد. ووضع ناتان فريتاس ومشروع غارديان في نيويورك تطبيقات لنقل الاتصالات المشفَّرة وتور إلى الهواتف المحمولة.

وموّلت الحكومة الأميركية بعض المشاريع، مثل تور، باسم حرّية الإنترنت، في حين كانت وزارة العدل تتحرى في الوقت نفسه، مع مطوِّر تور، يعقوب أبلبوم، عن تورّطه في ويكيليكس.

وسلك فيل زيمرمان، مؤسس بريتي غود برايفسي، طريق الرأسمالية. لقد باع بيي جي بيي لنتورك أسوشيتس عام 1997 لقاء مبلغ 36 مليون دولار. وفي العام 2012، انضم إلى جون كالاس، واضع كتابة مشفَّرة، وعضو في القوات الخاصة للبحرية الأميركية، مايك جانك، لوضع خدمةِ كتابة مشفَّرة تدعى الحلْقة الصامتة (Circle Silent) تبيع تطبيقاتٍ لنصوص واتصالات هاتفية مشفَّرة.

á á á

كان الحلْقة الصامتة برنامج التشفير الأسهل الذي استخدمتُه يوماً. كل ما عليّ القيام به هو تحميل تطبيقَين على هاتفي آي فون، هما سايلنت تكست (Text Silent) وسايلنت فون (Phone Silent)، فيشفِّر على الفور.

ولكنني كنت بحاجة إلى التحدث إلى أحدهم. فكلفة الخدمة تبلغ

9,95 دولاراً في الشهر، وكنت أجد صعوبة في العثور على من يرغب في التسجل.

أخيراً، أقنعتُ مصدراً حساساً بتحميل سايلنت تكست وسايلنت فون أيضاً. فجلسنا في حانة وقضينا ساعة في تحميل التطبيقات على هاتفَينا المحمولَين، وكنا حريصين على عملها. فاتخذتُ لي اسم آيدا، واتخذ مصدري له اسماً زائفاً.

لقد أرسلنا نصوصاً مرات قليلة بنجاح، حتى إننا أجرينا اتصالاً طويلاً على سايلنت فون. كان الاتصال مُجهِداً - بتأخيرٍ دام ثلاث ثوانٍ بين الكلام والنقل، ولكن الأمر نجح في الغالب. قال لي المدير التنفيذي الأعلى لسايلنت سيركل والمؤسس المساعد مايك جانك إن سبب التأخيرات يعود إلى استخدامي التطبيق على شبكة الهاتف المحمول بدلاً من الواي - فاي. (كنت قد أطفأت الواي - فاي لتجنّب عملية التعقُّب التجاري للمواقع). علاوةً على ذلك، أشار إلى أنني ومصدري لم نضغط على زر "تحقق" في بدء المكالمة، وهو إغفال قد يتسبب أيضاً باعتراض الاتصال.

ولكن عندما حاولتُ ومصدري تدبّر لقاء شخصي، توقفتُ فجأةً عن تلقّي إجابات عن نصوصي الصامتة، وكل ما كنت أرى رسالةً تقول "تحديد مفاتيح".

في وقت لاحق، سألتُ سايلنت سيركل عن هذا الحادث، فشرح لي التقنيّ الأعلى جون كالاس، قائلاً إن سايلنت تكست يتبادل مجموعة جديدة من المفاتيح بعد كل نص. يعني ذلك إرسال وتلقّي معلومات أساسية ثلاث مرات على الأقل قبل استهلال عملية وضع النصوص. لقد سمح هذا الأمر لسايلنت سيركل بالتخلص من مفاتيحي بعد كل دورة بطريقة مماثلة لتوجيه رسائل بشكل غير رسمي (Messaging Off-the-Record).

ولكن الطرفَين كانا بحاجة للعمل عبر الإنترنت كي يجري التبادل الأساسي الديناميكي. لقد وجدتُ أنني إذا كنت أو شريكي في سايلنت تكست في مصعد أو في منطقة خالية من إشارات الهاتف المحمول، قد لا تتم عملية التبادل الأساسي.

في هذه الحالة، لقد أطاح أحدنا - مصدري أم أنا على حد سواء - بمفتاح أثناء التبادل. ونتيجةً لذلك، لم تُرسَل نصوصنا. كان يُفترض بنا الالتقاء في المساء، ولكننا لم نكن قد حددنا زماناً ومكاناً بعد.

مع انقضاء النهار ببطء، أصبحت يائسة باطّراد. لقد أرسلت نصاً لمصدري في الصباح لأسأله عن مكان وزمان لقائنا. لم أحصل على أي

جواب. ومع حلول الظهر، بدأت أشعر بالقلق.

عند الثالثة وثلاث عشرة دقيقة بعد الظهر، كتبتُ، "لا تتردد بالاتصال أو بإرسال نص في شأن مكان لقائنا. آمل في تمكننا من إنجاح الأمر"، ومع ذلك، لم أتلقَّ أية إجابة. وبدأت بالقلق حيال ما إذا كان مصدري قد فقد اهتمامه باللقاء.

عند الخامسة وسبع دقائق مساءً، حاولتُ ثانيةً: "هممم - حصلتُ على إشعار بنص ولكنني لم أتلقَّ أي نص". مع ذلك، لا إجابة.

أخيراً، عند السادسة وأربع وعشرين دقيقة، اتصل مصدري بـي على الهاتف المحمول للتسجّل. لم ينجح التشفير. لقد عدنا إلى شبكة التعقُّب.

إنه لغز استخدام التشفير في عالم اليوم. فعندما ينجح الأمر، يكون الأمر سحرياً. وعندما لا ينجح، يكون النوع الأسوأ من الوعد الزائف، النوع الذي يمكنه خيانة العلاقات الحساسة.

á á á

واصلت استخدام سايلنت سيركل. فبالرغم من كل عيوبه، كان أقل إرهاقاً من برامج التشفير الأخرى التي أستخدم.

لقد أقنعتُ عدداً قليلاً من الأشخاص بالانضمام إليّ على سايلنت سيركل: صديق مقرَّب يُقيم في باريس؛ باحثةُ كتابـي المقيمة في اليابان؛ وزميلة محترفة.

وتعلّمتُ العيش مع مفاتيح محذوفة. كنت وصديقتي في باريس - واسمها على سايلنت سيركل هِدي لامار - نحذف مفاتيح في غالب الأحيان لدرجة إجرائنا اتصالات هاتفية أسبوعية نضغط خلالها على "مفتاح التصفير" في الوقت نفسه، مراراً وتكراراً، حتى تصفَّر مفاتيحنا أخيراً.

أخيراً، بتنا نعتبر معاً سايلنت تكست أقرب إلى موجِّه رسائل فورية منه إلى موجِّه نصوص. كان يتعيّن على كلَينا أن نكون على الإنترنت في الوقت نفسه. وإذا لم يكن أحدنا على الإنترنت، تُحذف مفاتيحنا في غالب الأحيان وتختفي رسائلنا في الأثير.

وكشف سايلنت تكست أيضاً عن هوَس هِدي الباطني بالإحراق. لقد وقعتْ في غرام ميّزة تسمح لها بـإحراق (burn) رسائلها، فتتلاشى أمام عينَيّ بعد أربع وعشرين ساعة من تلقّيها. من حين لآخر، كانت الرسائل تحترق قبل قراءتها. فتذمّرتُ، مُعربةً عن حاجتي إلى توثيق تبادلاتنا لأجل البحث الذي أُجريه لأجل الكتاب، ولكن ذلك حثّها على إحراق المزيد.

خلال إحدى زياراتها إلى نيويورك، قالت لي هِدي إن شكوكاً بدأت

تنتابها أخيراً في شأن إحراق كل الرسائل. "قرأت إحدى رسائلك وكان لديك إجابة ذكية"، قالت لي. "ولكن سبق لي أن أحرقت رسالتي كي لا أتمكن من تذكر ما كانت إجابتك الذكية".

لقد فكّرت مليّاً، ولفترة وجيزة، بعدم إحراق الرسائل، ولكنها قررت أخيراً مواصلة قذف بياناتنا في ألسنة لهب وهمية.

"إنه أمر لذيذ ومؤلم"، قالت. "ولكنها الحياة".

الفصل الرابع عشر
مقاومة الخوف

تتمثل مهمتي بمراقبة ابني وابنتي. إنه عمل متواصل - في كل دقيقة من حياتي أكون فيها مستيقظة أو نائمة، يُفترض بـي معرفة مكان وجود صغيرَيّ، ماذا يفعلان، وكيف يبقيان آمنَين. كما يعلم كل والد ووالدة، إنه عمل مُرهِق. فتعقُّب صغار في الأرجاء ليس عملاً جسدياً مُرهقاً فحسب، بل مُجهِداً ذهنياً أيضاً عندما تعرفون أنكم مسؤولون عن كل ما يحدث - سواءً أكان خطأكم أم لا. وإذا صودف نظري إلى هاتفي المحمول أثناء خروج صغيرَيّ ركضاً إلى الشارع وصدْم سيارة لهما (لا سمح الله)، لن ألوم نفسي فقط بل إن كل شخص في العالم سيُلقي باللائمة عليّ أيضاً.

إنه نوع الضغط الذي قد يدفع شخصاً ما إلى اتخاذ تدابير صارمة: تكبيل الصغار، أو مراقبتهم سرّاً بواسطة برنامج تجسسي، أو تركيب كاميرات لمراقبةِ جليسة الأطفال.

في الواقع، يُختصر الكثير من النُّصح المقدَّم من قِبَل الخبراء في شأن حماية خصوصية الصغار بـ"مراقبة صغاركم".

- توصي الأكاديمية الأميركية لطب الأطفال بإشراف الأهل على صغارهم كلما استخدموا جهاز كمبيوتر، واستخدام برنامج لتعقُّب مواقع الويب التي يزورها صغارهم، والتفكير ملياً في استخدام برنامج رَقابة لصدّ ولوج مواقع الويب غير المقبولة.
- توصي الأف بـي آي باستخدام الأهل برنامجَ صَدّ "ومواصلة ولوج حساب صغيركم على الإنترنت والتحقق عشوائياً من بريده/أو بريدها الإلكتروني".
- تقترح وزارة الأمن الداخلي استخدام برنامج لمراقبة مواقع الويب التي يزورها الصغار. "يمكن استخدام أدوات المراقبة سواءَ عرف الصغير بالأمر أم لا".

أستطيع فهم سبب اتّباع العديد من الأهل هذا النُّصح. بالرغم من كل شيء، يأتي النُّصح من مصادر شرعية. فالأهل يخافون عالَماً مفزِعاً، ويأملون في أن تساعدهم الرَّقابة على الحؤول دون وقوع كارثة.

أتخيّل أن يكون ذلك الشعور الوالديّ نفسه حافزاً للمدراء التنفيذيين في وكالة الأمن القومي. فمهمتهم تتمثل بحماية الأمّة، وهم يعرفون أنهم

سيُلامون إذا وقع حادث إرهابـي. لذلك، يقررون مراقبة كل شيء - تحسّباً.

ولكنني لا أستطيع تبرير إعداد شبكات تعقُّب لمراقبة كل خطوة يقومان بها أثناء محاولتي الإفلات من رَقابة شبكة التعقُّب. فأقل ما يُقال في ذلك إنه عمل نِفاقيّ.

á á á

لماذا لا نستسلم؟ لماذا لا ندسّ رُقاقة جي بيي أس في حقائب ظهر صغارنا؟ لماذا لا نثبّت برنامجاً جاسوسياً في كمبيوتراتهم لمراقبة كل نقرة على الفأرة؟ ألن يكون صغيراي أكثر أماناً؟

ربما. ولكن يجدر التذكُّر أن صغيرَيّ آمنان تماماً في الواقع. لقد هبطت الجريمة بشكل عمودي في الولايات المتحدة في السنوات العشرين الماضية. وانحدر معدل الجريمة العنيفة بنحو 40 بالمئة بين عامَي 1990 و2009. وانخفضت جرائم الأملاك بنحو 40 بالمئة. وتراجعت سرقات المركبات الآلية بنسبة تزيد عن 50 بالمئة.

في مدينة نيويورك حيث أعيش، إن الأرقام مثيرة أكثر فأكثر. لقد انخفضت الجرائم بنسبة 83 بالمئة منذ العام 1993، وانخفضت أعمال السَّلب بنسبة 78 بالمئة، وسرقة البيوت بنسبة 83 بالمئة. وسجلت المدينة ثاني أقل معدّل للجريمة بين المدن الكبيرة إذ بلغ 5,05 جريمة قتل لكل 100,000 شخص عام 2012. في سان دييغو فقط، كان المعدل أكثر انخفاضاً بين المدن التي يزيد عدد سكانها عن مليون نسمة، وبلغ 3,51 لكل 100,000 شخص.

لقد انخفضت أيضاً الجرائم المرتكَبة بحق الأطفال. فهبطت الإساءة الجنسية للأطفال بشكل عمودي في الولايات المتحدة بين عامَي 1992 و2010، وفقاً لمجموعة دراسات حلّلها مركز أبحاث الجرائم ضد الأطفال. وتُظهر دراسات أخرى أن التنمّر في انحدار أيضاً، عِلماً أن معدلاته ما تزال أعلى مما ينبغي. وانخفضت حالات الانتحار والحَمْل في سنّ المراهقة في الأعوام العشرين السابقة. ويُظهر البحث باستمرار أن الجرائم ضد الأطفال تُرتكَب في الغالب من قِبَل أشخاص يعرفونهم.

إذاً، لماذا يوجد هذا الإحساس بأن عالمنا المتخَم رقمياً خطِرٌ جداً لدرجة الحاجة إلى مراقبة الصغار؟ يدعو ديفيد فينكلهور، مدير مركز أبحاث الجرائم ضد الأطفال، الحاجةَ إلى مراقبة الصغار ذُهاناً ارتيابياً، والحاجةَ إلى مراقبة الإنترنت "ذُهاناً صبيانياً". هو يقدّر أن يكون الذُّهان الصبيانيّ ناجماً عن واقعِ شعورِ الأهل العصريين بأنهم يواجهون ثقافة شعبية. في الماضي،

كانت عائلات تعيش في مجتمعات وقبائل أصغر حجماً حيث تتشاطر قِيَماً مع عائلات أخرى. اليوم، غالباً ما يشعر الأهل العصريون بأنهم يكبحون موجةَ ثقافةٍ شعبية تحتفي بالجنس، بالطعام غير المغذّي، بالعنف، وبالروح الاستهلاكية. "أنه أمر مثير للسخرية، ولكن الأهل في البيئات الأكثر نُخبوية في أميركا يائسون، على غرار الجميع، لحماية أبنائهم وبناتهم من تيار التأثير الثقافي"، يكتب فينكلهور.

وهكذا، فخوف الأهل ليس من الجريمة فحسب، بل أيضاً من تأثير الأفكار الفاسدة خارج المنـزل. هل هو سبب كافٍ لإجراء رَقابة؟

إنه سؤال صائب بعد أن فهمتُ الآثار النفسية للرَّقابة. يُظهر بحث أن الرَّقابة السرّية قد تتسبب بالقلق والكبت الذاتي لدى البالغين. لدى الصغار، تُحدث الرَّقابة كآبة بصفة خاصة، كما يبدو: هي تقوّض حماستهم للتعلم.

لقد استنتجت دراسة مِفصلية عام 1975 أن لِرَقابة البالغين للصغار أثرَ "تحويل اللعب إلى عمل"، مما يُثبط حماسة الصغار للّعب بأُحجية مشوِّقة. في الدراسة، تُرك الصغار بمفردهم في غرفة مع كاميرا موجَّهة نحوهم، وقيل لهم إن بالغاً سيراقبهم عبر الكاميرا أثناء اللعب بأُحجية. عندما قُدِّمت الأُحجية، في المرة التالية، للصغار المراقَبين في غرفة صف غير مزوَّدة بكاميرا، بدوا أقل اكتراثاً من مجموعة المراقبة باللعب بالأُحجية. "إن معرفة قيام شخص ما بمراقبة وتقييم أداء شخص آخر... تبدو كافية لتخفيض اهتمام الأخير بالمهمة"، كتب مؤلّفا الدراسة مارك أر. ليبير وديفيد غرين.

انخفض اهتمام الصغار بالأُحجية أكثر فأكثر عندما مُنحوا مكافآت جليّة بسبب لعبهم بالأُحجية. وعُرضت على الصغار ألعاب مُغوية، وقيل لهم إن بإمكانهم اللعب بها إذا أجادوا اللعب بالأُحجية. وعندما قُدمت لهم الأُحجية، في المرة التالية، في غرفة صف غير مزوَّدة بكاميرا، انخفض اهتمامهم بالأُحجية أكثر فأكثر. واستنتج ليبير وغرين أن الطريقة الفضلى لإثارة اهتمام الصغار بنشاط ما تتمثل "بممارسة أقل قَدْر من الضغط الكافي لإثارة السلوك المرغوب فيه أو المحافظة عليه".

á á á

حتى قبل اهتمامي بالخصوصية، اعتبرت أنه من الجائر نشر أية صور لصغيرَيّ على الإنترنت. لم أعتقد أنه من المنصف لي بناء أثر رقمي لهما يتعيّن عليهما التعاطي معه في وقت لاحق.

فمنذ ولادة صغيرَينا، أتشاطر وزوجي على الدوام صوراً للصغيرَين بشكل سرّي. في بادئ الأمر، استخدمنا موقع كوداك غالري (Kodak Gallery)، غير المستعمَل الآن، لإرسال محتويات صور شفافة لعائلتنا والأصدقاء. للأجداد، كنا نطبع بانتظام صوراً ونرسلها على الورق. ولكننا كففنا عن استخدام كوداك غالري عندما بدأ يهدد بمحو صورنا إذا لم نشترِ ما يكفي من الصور في غالب الأحيان.

بعد التخلي عن كوداك غالري، استخدمنا لمدة وجيزة خدمة أخرى لتشاطر الصور هي شاترفلاي (Shutterfly). ولكننا أدركنا في النهاية أن تَشاطُر الصور عملية محدودة. فعدد قليل من الأشخاص فقط يريدون رؤية صورٍ لامتناهية للأطفال. لذلك، شرعنا بإرسال صور للأجداد عبر البريد الإلكتروني، وصور قليلة أخرى للأنسباء.

بالرغم من ذلك، كانت هناك سهوات قليلة عندما ترسَل صورة ما للعلَن. عندما وُلد ابني عام 2008، كنت منهَكة جداً ويتعيّن عليّ إبلاغ عدد كبير من الأشخاص بنشري صورة له على فيسبوك. ما تزال تلك الصورة هناك - ويُزعجني ذلك. لقد محوتها، ولكنها ما تزال في البيانات التي حمّلتُها من فيسبوك.

لقد أنـزل زوجي ذات مرة، عن طريق الخطأ، صوراً للعائلة على غوغل+ عندما اعتقد أنه يسجّل دخوله ليس إلا إلى حسابه على بريد غوغل الإلكتروني. كان قادراً على محوها، ولكن اختفاءها عن نتائج بحث غوغل تطلّب بعض الوقت.

في مرة أخرى، نشرت والدتي صورة لابنتي ولي ببيجامتَينا (!) على مدوّنتها دون أن تأخذ رأيي. فلاحظت ابنتي الصورة وطلبت من الجدة إزالة الصورة. فأزالتها الجدة، ومرة أخرى، تطلّب اختفاؤها عن نتائج بحث غوغل بعض الوقت. ولكنها زالت الآن.

ولكن ليس من السهل ضبط صور صغيرَيّ الرقمية. فكل مخيّم صيفي ونشاطٍ يُقام بعد المدرسة يترافق مع استمارة تطلب مني السماح لهم بالتلقاط صور لصغيرَيّ واستخدامها كما يحلو لهم. أرفض التوقيع، ولكنني أكره أن أكون والدة مُزعجة مثيرة للمتاعب.

أعرف أنها معركة خاسرة. فكما أنه لا يمكنني الحؤول دون التقاط صور لي في العلن، لا يمكنني الحؤول دون عيش صغيرَيّ في عالَم مُتخَم بالكاميرات. ولكن يبدو أنه من الظلم عدم امتلاكي أية حقوق في شأن صور صغيرَيّ. فإذا إراد أحدهم تصوير صغيرَيّ على شريط تسجيل فيديويّ

علناً ونشر الفيديو على الإنترنت، لا أملك أي حق قانوني بإزالته. ولكن إذا كان الفيديو يحتوي على موسيقى محفوظة الحقوق، يمكن لمالك حقوق الطبع والنشر إزالتها بسرعة البَرق.

فسألتُ عدداً قليلاً من المحامين، بإيجاز - وعلى سبيل المزاح في الغالب، عما إذا كان بإمكاني الحصول على حقوق طبع ونشر صور صغيرَيّ. قالوا إنه لا يمكنني القيام بذلك.

وهكذا، أواصل محاولة إبقاء الصور خارج الإنترنت، عِلماً مني بأنني سأُخفق في نهاية المطاف.

á á á

هناك قانونان يُفترض بهما حماية خصوصية الأطفال: قانون حماية خصوصية الأطفال عبر الإنترنت - كوبا (COPPA) وقانون الخصوصية والحقوق التربوية للعائلة - فيربا (FERPA). ولكن أيّاً منهما ليس فعالاً بصفة خاصة.

في الواقع، وقبل شروعي باختبارات الخصوصية، انتهكتُ قانون حماية خصوصية الأطفال عبر الإنترنت العائد للعام 1998. يطلب القانون من مواقع الويب الحصول على إذنٍ والديٍّ قبل جمع معلومات شخصية عن الأطفال الذين هم دون سن الثالثة عشرة. وفي العام 2013، طُوِّر القانون ليشمل نوع المعلومات التي تتطلب موافقةً والديّة كي تُستخدَم في عملية التعقُّب السلوكي، والصور، وشرائط الفيديو، والموقع، عبر الإنترنت.

يهدف كوبا إلى منع مواقع الويب من استغلال الصغار. ولكن القانون يُثني الشركات أيضاً، لسوء الحظ، عن بناء مواقع ويب مخصَّصة للصغار الذين هم دون سن الثالثة عشرة لأنها عندما تملك "معلومات فعلية" عن استخدام الصغار لمواقعها، يكونون بحاجة للحصول على إذن والديّ.

نتيجةً لذلك، تُشجّع كوبا الكذب. لقد أعددتُ لابنتي حساباً على بريد غوغل الإلكتروني عندما كانت في سن السابعة - عِلماً أن بريد غوغل الإلكتروني يقتضي أن يكون المستخدمون في سن الثالثة عشرة. لقد أردناها أن تكون قادرة على توجيه رسائل بريد إلكتروني لجدَّيها المقيمَين في الهند.

دفاعاً عن نفسي، لست الوالدة الوحيدة التي تكذب في شأن سن صغيرتي على الإنترنت. ففي العام 2011، قيّم باحثون بقيادة دانان بويد، من مايكروسوفت، أكثر من ألف والدِ طفلٍ تتراوح أعمارهم بين العاشرة والرابعة عشرة، ووجدوا أن ثلثهم قالوا إن صغارهم يملكون حسابات على فيسبوك قبل بلوغهم سن الثالثة عشرة، وثلثَي الأهل ساعدوا صغارهم على

إعداد حسابات. واستنتج الباحثون أن قيود السنّ وفقاً للقانون "ليست حلاً للخصوصية وللمخاوف المتعلقة بالحفاظ على السلامة عبر الإنترنت، وليست وسيلة لتخويل الأهل اللجوء إلى القانون".

وصُمِّم قانون الخصوصية والحقوق التربوية للعائلة العائد للعام 1974 لمنح الأهل حق ولوج سجلات أطفالهم التربوية والحصول على موافقةٍ والديّة قبل تحويل تلك السجلات إلى طرف ثالث. ولكن فيربا مليئة بالثغرات: يمكن للمدارس تسليم السجلات "لمسؤولي المدرسة" أو "لمنظمات تُجري دراسات لصالح المدرسة" دون موافقةٍ والديّة. وتُعتبر معلوماتٌ عن اسم الطالب، وعنوانِه، وعنوان بريده الإلكتروني، ورقم هاتفه، ووزنه، وطول قامته، وصور فوتوغرافية له، "معلوماتٍ توجيهية" يمكن الكشف عنها دون إذنٍ والديّ.

في نيويورك حيث أقيم، ترسل المدارس العامة بيانات الطلاب إلى مركز خارجي لتخزين البيانات يدعى إينبلوم، ويُقال إنه يهدف إلى مساعدة المدارس على تطوير تكنولوجيا تروّج "للتعليم الذي يُضفى عليه طابع شخصي". كما يبدو، سيسمح هذا النوع من التعليم "للمدرسين بالاضطلاع بدور المدرسين الخصوصيين، وللطلاب بالتعلّم وفقاً لقدراتهم الشخصية، وللتكنولوجيا بتتبّع تطوّر الطلاب، وبالحكم على المدارس بالاستناد إلى النتائج التي يقدّمونها". لأجل هذا الحُلم، بإمكان نيويورك البدء بدفع ما بين دولارَين وخمسة دولارات لإينبلوم لقاء كل صغير عام 2015.

أفضّل إنفاق ذلك المال على رواتب وكتب دراسية بدلاً من وهب بيانات صغيرَيّ لقاعدةِ بيانات قاعةِ مرايا ذات قيمة غير مُثبَتة ومشكوك فيها. ولكنني لا أستطيع محو المعلومات المرتبطة بصغيرَيّ من قاعدة البيانات. لا وجود لاختيارِ عدم الاشتراك في فيربا إذا كانت المدرسة تريد مشاطرة بيانات مع "منظمات تُجري دراسات"، عِلماً أن باستطاعة منطقة إدارة مدارس ميسورة إنشاء اختياراتها الخاصة لعدم الاشتراك إذا رغبت. يقول مركز إينبلوم الذي لا يبتغي الربح إنه لا يرى بيانات الصغار، أو يستخدمها، أو يحللها، أو يبيعها.

بأسف، يجب عليّ الاستنتاج أن أيّاً من قانونَي خصوصية الأطفال لا يخدمني بشكل جيد.

á á á

تقول حكمة تقليدية إن الصغار لا يأبهون بالخصوصية. ويقول بالغون باستمرار إن الخصوصية مسألة جيليّة والصغارُ سعداء تماماً بعيش حياة

علنية تماماً.

وصحيح أن الصغار ارتكبوا أخطاء فادحة في نشر أمور خرقاء على الإنترنت - مع عواقب وخيمة أحياناً.

تأمّلوا بجاستن كارتر من تكساس، البالغ من العمر ثمانية عشر عام، والذي اعتُقل بسبب تدوين تعليق ساخر على صفحة فيسبوك خاصة به. كان كارتر وصديقه يتناقشان حول لعبة الفيديو على الإنترنت ليغ أوف لجندس، فدعاه صديقه مجنوناً. وكتب كارتر يردّ عليه: "أعتقد أنني سأطلق النار على روضة أطفال وأشاهد دم الأبرياء ينهمر، وآكل القلب النابض لأحدهم". لقد اعتُقل واتُّهم بتوجيه تهديد إرهابـي. سُجن كارتر من شباط/فبراير حتى تموز/يوليو 2013 قبل قيام مانحٍ غُفل بدفع الكفالة البالغة 500,000 دولار التي لم تتمكن عائلة كارتر من تدبّرها.

ولكن يجدر التذكُّر أن البالغين يكتبون أموراً غبية عديدة على الإنترنت أدت إلى عواقب وخيمة أكثر مما ينبغي. تأمّلوا بهاتَين القصتَين.

- في كانون الثاني/يناير 2012، أُلقي القبض على سائحَين بريطانيَّين لمدة اثنتَي عشرة ساعة أنكرا دخولهما إلى الولايات المتحدة بعد إطلاق أحدهما تغريدة عن الرحلة الوشيكة: "أنا غير منشغل هذا الأسبوع، سأُطلق بعض الشائعات قبل أن أذهب لأدمّر أميركا"، في إشارة إلى "الاحتفال" في الولايات المتحدة.
- في 9 أيلول/سبتمبر 2009، كان لجو ليباري اختبار سيّئ في أحد متاجر أبل في نيويورك. وعندما وصل إلى المنـزل، أعاد صياغة اقتباس من فايت كلوب على صفحة آرائه المنشورة على فيسبوك، وجاء فيه، "قد يدخل جو ليباري متجراً لأبل في الجادة الخامسة مع سلاح نصف أوتوماتيكي يعمل على الغاز من طراز أرماليت أيه أر -10 ويُطلق النار مراراً وتكراراً على أولئك النواطير المغرورين المخبولين". بعد أقل من ساعتَين، كان ضباط قسم شرطة نيويورك عند بابه. لقد فتّشوا منـزله بحثاً عن متفجرات، واعتقلوه، واتهموه بتوجيه تهديدات إرهابية. فقاوم الاتهامات لمدة عام، رافضاً القيام بمساومة دفاعية حتى أُسقطت الاتهامات أخيراً.

يُظهر بحث أن الصغار يهتمون بالخصوصية حقاً. ففي العام 2012، وجدت معاينة دقيقة لمراهقين يستخدمون تطبيقات على هواتفهم الذكية أن 46 بالمئة منهم أطفأوا مميّزات تعقُّب المواقع على هواتفهم، و26 بالمئة أزالوا تطبيقاً بسبب مخاوف مرتبطة بالخصوصية. ووجدت الدراسة أيضاً أن 70 بالمئة من المراهقين طلبوا نُصحاً حول كيفية إدارة خصوصيتهم على

الإنترنت.

حتى إن الصغار الذين لا يبدون مهتمين بخصوصيتهم غالباً ما يلجأون إلى خِدَع لحماية أنفسهم على شبكات التواصل الاجتماعي، وفقاً لمقابلات أُجريت مع 163 مراهقاً قامت الباحثتان في مايكروسوفت، دانا بويد وأليس مارويك، بتحليلها. وتصف الباحثتان مناورة ماكرة قامت بها فتاة في السابعة عشرة من عمرها تدعى كارمن ناضلت للتواصل مع صديقاتها على فيسبوك، عِلماً أن والدتها صديقة على فيسبوك.

كانت كارمن حزينة بسبب انفصال، فنشرت على فيسبوك كلمات أغنية من "انظروا دائماً إلى الجانب المُشرق من الحياة". فسّرت والدة كارمن الكلمات حرفياً وعلّقت، قائلةً إن كارمن تُبلي بلاءً حسناً كما يبدو. ولكن صديقات كارمن فهمنَ المعنى الضمنيّ لكلمات الأغنية: ظهرت الأغنية في الفيلم السينمائي حياة براين حيث كانت مونتي بايثن الشخصية الرئيسية في مواجهة الصَّلب.

وتردد صدى رسائل كارمن الضمنية في عقلي. بالعودة إلى سنواتي في المدرسة الثانوية، لم يكن لدينا فيسبوك. فالمساحة الوحيدة لنشر آرائنا كانت الكتاب السنوي. ففي نهاية كل عام، يتعيّن على كل طالب في الصفوف العليا تزيين صفحة من الكتاب السنوي. كانت صفحتي - وصفحات آخرين عديدين - مزيجاً من دُعابات طلاب وكلمات أغانٍ مبهَمة.

لقد نقّبتُ في صفحة كتابـي السنوي وتفقّدتُ رسائلي. لم أتمكن من فك شيفرة معظمها. لماذا صرختُ في وجه صديقتي هيدي، قائلةً "ورقة سائلة"؟ وماذا عنيتُ عندما طلبت من صديقتي سوزي "القيام بنـزهة على الأقدام على الجانب المعتدل؟" ماذا حدث في 15 آب/أغسطس وأردت تذكُّره مع صديقتي شيرلي؟ كل شيء ضائع في رمال الزمن.

ولكن الرسائل الضمنية كانت فعالة في ذلك الوقت، وتعرف صديقاتي ما أعني، ووالداي محيَّرَين بقدر حيرتي الآن.

في الواقع، طالما أثارت الخصوصية اهتمامي، حتى في سن المراهقة. في صِغَري، كنت قلقة من الرَّقابة الوالدية. الآن، أنا قلقة من رَقابة الشركات والرَّقابة الحكومية.

على مَرّ الوقت، تغيّر ببساطة معيار رفع مستوى أمني الكمبيوتري إلى الدرجة الفُضلى.

á á á

عندما شرعتُ باختباراتي حول الخصوصية، اعتبر صغيراي الخصوصية

تحدياً يتعيّن عليهما التغلب عليه.

لقد أطلقتُ على ابنتي لقب هارييت الجاسوسة لأنها تجيد التجسس عليّ. ذات مرة، كنت أعمل في المنـزل وعادت ابنتي من المدرسة بعين زهرية اللون. كنت في الغرفة أتحدث عبر الهاتف إلى صديقة وأشكو من كيفية عدم تمكّني من تشغيل جهازي الحضني، ماك، على مرقاب هيولت - باكرد عندما وصل هذا البريد الإلكتروني:

كنت أسمع كل كلمة تقولينها عن كيفية عدم انسجام جهازك الماك مع إيتش - بيي. لقد سمعتُ أكثر من 10 لعنات ومعظمها "تبّاً".

فتحتُ باب غرفة نومي، ورأيت ابنتي حاملةً الآي باد وتقهقه بسبب نجاحها في استراق السمع. كانت تحب أيضاً اختلاس النظر أثناء قيامي بإدخال كلمات مروري.

يعتقد صغيراي أيضاً أنني شريرة بسبب عدم السماح لهما بنشر أفلام فيديو على يوتيوب. فابنتي في التاسعة من العمر، وابني في الخامسة. هما يحبان الإنترنت، ولا سيما يوتيوب. لقد علّمتْ ابنتي نفسها العزف على البيانو من خلال مشاهدة يوتيوب. وأُغرم ابني بموسيقى وودي غاثري عندما عثر عليها على يوتيوب. (يحب أن أدعوه وودي في هذا الكتاب، لذلك سأفعل).

يحلم هارييت وودي بنشر أفلامهما الفيديوية الخاصة على يوتيوب. بالرغم من كل شيء، هكذا تُجرون حواراً في عالم اليوتيوب. يقوم شخص ما بنشر فيديو، فينشر آخر فيديو يعتمد على الأول أو يستجيب له. وصغيراي مُحقّان في أن تَشاطُر الفنانين أعمالهم هي الطريقة لتطوّر الفن. فيوتيوب هو مقهى باريس في زمنهم، وأشعر بأنني سيّئة جداً في شأن إنكاري عليهما حق الاستمتاع بهذه التبادلات المبدعة.

ولكنني لا أستطيع وعدهما بعدم عودة تلك الأفلام الفيديوية - أو نشاط آخر عبر الإنترنت - لتلازمهما يوماً ما. يمكن استخدام ذلك لحرمانهما من عمل أو جواز سفر، أو لحرمانهما ببساطة من حق تحديدهما نظرة العالَم إليهما.

عندما أفكر في طفولتي، أشعر بأنني مبارَكة لأن حياتي تكاد لا تكون موثَّقة. فبدون آثار رقمية، كنت قادرة على إعادة ابتكار نفسي تماماً متى شئت. في المدرسة الثانوية للأحداث، مثلاً، كنت أرتدي ملابس زهرية اللون وفيروزية اللون فقط. ولكن عندما انتقلت إلى الجانب الآخر من المدينة لارتياد المدرسة الثانوية، غيّرت مجموعة ملابسي كلّياً وارتديت ملابس

كلاسيكية مع أحذية بِني لوفر. لم يعلم أحد بتحوّلي بسبب عدم وجود أثر لي، باستثناء عدد قليل من الصور الفوتوغرافية الشاحبة في علبة حذاء في خزانة والدَيّ.

أريد لصغيرَيّ أن ينعما بالحرية نفسها لإعادة ابتكار نفسَيهما. ولكنني أدرك أن قول "لا" طوال الوقت سيحملهما على كنّ الكره للخصوصية ومحاولتهما التحايل عليّ.

á á á

قررت اعتماد مقاربة جديدة. فبالاستناد إلى صفحة في الدراسة تتناول تحويل "اللعب إلى عمل"، سأحاول تحويل الخصوصية إلى لعب.

لقد قررت التعاطي مع أدوات الخصوصية كما لو أنها ألعاب جذّابة يملك صغيراي فرصة اللعب بها، دون مكافآت صريحة أو رَقابة على أعمالهم.

كانت مهنة كلمة المرور بداية رائعة. لقد أحبت ابنتي جني المال من رمي النَّرد وبيع كلمات مرور منيعة، وأحبت كون الأمر نشاطَ شخص بالغ؛ لقد تأثر البالغون عندما أخبرتهم عن مهنة كلمات المرور، وكانوا أكبر زبائنها.

بعد شروع هارييت بمهنة كلمات المرور، كفّت عن محاولة اختلاس النظر إلى كلمات مروري، وكان ذلك بمثابة علامة إضافية لي. كانت تعرف أنها مخزَّنة في 1باسوورد أم أنها نسخات معدَّلة لكلمات المرور التي أعدّتها لي. لقد تغيّرت اللعبة بالنسبة إليها: باتت اللعبة الآن وضع كلمات مرور أفضل، وليس كشف النقاب عن كلمات مروري.

وسرعان ما أصبحت هارييت فضولية في شأن اختباراتي الأخرى حول الخصوصية. كانت تحب هويتي الزائفة التي تحمل اسم آيدا تاربيل، وقررتْ اعتماد اسمها الزائف لأجل حساباتها على الإنترنت أيضاً. فأيٌّ من الصغيرَين ليس كبيراً بما يكفي كي تكون له نِبذة على مواقع التواصل الاجتماعي، ولكن هارييت غيّرت عنوان بريدها الإلكتروني بما يتناسب مع اسمها الزائف. بالرغم من كل شيء، ستعرف صديقاتها والعائلة بأنها هي. لا يعدو الأمر كونه قليلاً من إخفاء معلومات اجتماعية.

وأدركت أيضاً أن لا سبب لعدم إشراك هارييت في التشفير. لذلك، أعددت لها حساباً على سايلنت سيركل على جهاز آي باد. كانت هارييت وآيدا تتبادلان نصوصاً مشفَّرة واتصالات هاتفية.

لقد أُثير اهتمام هارييت أيضاً بمحاولاتي صدّ أعمال التعقُّب عبر

الإنترنت. فوقفت بجانب جهازي الكمبيوتري وضحكت أثناء محاولتي تصفّح الويب باستخدام نوسكرييت المُربِك، مما زاد من صعوبة تحميل صفحاتي بشكل صحيح. وابتهجتْ عندما انتقلتُ إلى غوستري وظهر عدد أقل من الصفحات. كانت تحب بصفة خاصة شعار غوستري - شبح صغير أزرق ظريف يقبع في الزاوية اليمنى العليا لمتصفّح الويب. سرعان ما أرادت استخدام غوستري أيضاً.

وهكذا، أنـزلتُ غوستري على جهازها، وهو كمبيوتر محمول قديم حصلنا عليه مجاناً عندما حصلنا على إنترنت فائق السرعة. وبدأتْ باعتبار غوستري لعبة فيديو بهدف العثور على مواقع ويب يلجها معظم المتعقِّبين. "يا أمي، عثرتُ على موقع مع واحد وأربعين متعقّباً!" قالت لي، داخلةً إلى غرفتي رَكضاً مع الكمبيوتر.

حتى إن هارييت بدأت تحب داك داك غو ببطته المبتهجة مع ربطة عُنُق على شكل فراشة. لقد أعددتُه لها كمحرّك بحث افتراضي، واستمتعتْ بعرض البطة على صديقاتها.

ولكنها شكت من بطء تطبيق غوستري الشديد - الذي يستخدم محرك بحث داك داك غو - على آي باد. وبعد شهر من التذمّر، أخرجتُ أخيراً ساعة توقيت وقسنا الوقت. لقد تطلب البحث عن "جوائز غرامي" على تطبيق غوستري 6,7 ثوانٍ، في حين أن البحث نفسه دام على متصفّح سافاري من أبل 1,7 ثوانٍ. هي مُحقة. كان تطبيق غوستري بطيئاً جداً على آي باد.

لذلك، كففنا عن استخدام غوستري على آي باد، وأنـزلنا معاً ديسكونكت كيدس (Kids Disconnect)، وهو تطبيق لآي باد وضعه براين كينيش، مهندس غوغل الذي أطلق ديسكونكت عام 2010. فـديسكونكت كيدس يعتمد في الأساس التكنولوجيا نفسها التي كنت أستخدم عندما سمحتُ لأشكان سلطاني بتمرير حركة اتصالاتي على الويب عبر أجهزته الكمبيوترية كي يتحقق من المتعقّبين. قام ديسكونكت كيدس بالشيء نفسه - التقط كل حركة الاتصالات المغادرة من آي باد وصدّ أي اتصال بقائمة شركاتٍ شهيرة متعقِّبة للهواتف المحمولة.

لقد اعتبرتُ الأمر ذكاءً تاماً، ولكن أمل هارييت خُيِّب بسبب خلوّ التطبيق من المظهر الفيديوي. لم تتمكن من رؤية عدد المتعقِّبين الذين تم صدّهم لأنه يعمل بطريقة غير مرئية.

بعد قيامها باستخدامه لبعض الوقت دون توقف أيٍّ من تطبيقاتها

عن العمل، قررتُ تثبيت ديسكونكت كيدس على هاتفي الـآي فون. بالرغم من كل شيء، كنت أناضل لإيجاد طريقة لصدّ التعقُّب الإعلاني على هاتفي - وكان الحل الأفضل حتى ذلك الحين.

الآن، كلما ألقيت نظرة سريعة على روبوت ديسكونكت كيدس الأخضر الراقص على هاتفي، تعود إليّ ذكرى مواجهتي وصغيرَيّ التحديات نفسها لدى حماية أنفسنا من شبكات التعقُّب.

لا حاجة في الواقع للتمييز بين برنامج لحماية الخصوصية خاص بالـ"صغار" والـ"بالغ" عندما نُجرَف بأجمعنا بطريقة غير مميِّزة.

الفصل الخامس عشر
مبدأ عدم الإنصاف

في نهاية عامي الذي حاولت فيه الإفلات من الرَّقابة، شعرت على نحو مفاجئ بأنني مُفعمة بالأمل.

على أحد المستويات، لم تكن جهودي للإفلات من شبكات التعقُّب ناجحة جداً. لم أجد طريقة لاستخدام هاتفي المحمول - أو هاتفي "الخادع" - بطريقة تحمي موقعي وأنماط الاتصالات، دون بلوغ حد ترك الهاتف في المنـزل أو وضعه في قفص معدنيّ وقائيّ يجعله بلا فائدة. لم أخلّص نفسي كلّياً من قبضتَي غوغل وفيسبوك، وكان اسمي وعنواني ما يزالان موجودَين لدى أكثر من مئة وسيط بيانات لم يوفّروا لي إمكانية اختيار عدم الاشتراك. لم أكن قادرة على تجنّب كاميرات تمييز الوجوه.

ولكنني تجاوزتُ توقعاتي على صعيد آخر.

لقد تجنّبت الغالبية العظمى من التعقُّب الإعلاني عبر الإنترنت. كانت كلمات مروري - التي أعدّتها ابنتي من خلال رمي النَّرد واختيار كلمات من مُعجم - جيدة جداً. وسمحت لي هويتي الزائفة باسم آيدا تاربيل بالنأي بهويتي الحقيقية عن مشتريات حساسة، وبعض الاتصالات الهاتفية، ولقاءات شخصية. وتمكنتُ من إقناع بعض صديقاتي ومصادري بتبادل نصوص مشفَّرة، ورسائل فورية، وبريد إلكتروني.

لقد حققتُ نجاحي الأكبر مع صغيرَيّ، وهو أمر مفاجئ. كانوا قد بدأوا يفكرون بأن الخصوصية كلمة أخرى لـ"لا"، ولكن على مَرّ الزمن، بلغا مرحلة اعتماد تكنولوجيا لحماية الخصوصية تتراوح بين صدّ التعقُّب عبر الإنترنت والتشفير. حتى إنني تساءلت عما إذا كنت قد ذهبت بعيداً عندما وبّختني ابنتي بسبب إدخال رقم ضمانها الاجتماعي على استمارة المدرسة.

بالطبع، كانت نجاحاتي مؤقتة ليس إلا. ستسهّل التكنولوجيا تفكيك كلمات مروري الجديدة المؤلَّفة من عشرين مكوِّناً. وكلما استخدمت وصغيراي هويات زائفة، ازدادت سهولة إعادة ربط تلك الهويات بنا. وتخزَّن أحاديثي المشفَّرة، على الأرجح، من قِبَل وكالة الأمن القومي كي يتم تحليلها في وقت لاحق. ويطوّر المتعقّبون الإعلانيون عبر الإنترنت تكنولوجيا جديدة للتحايل على تقنياتي الصادّة.

ولكنني أدركت أن لا قيمة للمحاولة. فاختياراتي لعدم الاشتراك دليل إضافي ينقض حجة وسطاء البيانات بأن عدداً قليلاً من الأشخاص يهتمون بالخصوصية ويختارون عدم الاشتراك. واستخدامي للتشفير وبرامج إخفاء الهوية يُنبئ وكالة الأمن القومي وشركات الإنترنت بأنني لا أريدهم قراءة رسائلي، وقد شجعتُ بعض صديقاتي وزملائي للانضمام إليّ في اعتماد الكتابة المشفَّرة. وشجّع استخدامي لهويات زائفة صغيرَيّ لتطوير استراتيجياتهما الخاصة في اعتماد أسماء مستعارة، وكلّي أمل في أن يساعدهما ذلك في سنوات المراهقة.

باختصار، بلغتُ حد الاعتقاد بأن أعمالي كانت فعالة، على الأرجح، في إدخال تعديلات على النقاش الذي يتناول الخصوصية أكثر من فعاليتها في مواجهة الرَّقابة. لقد ذكّرتني أعمالي باعتصامات منضدات الغداء في الستينات، عندما جلس طلاب سود في غرينسبورو، كارولاينا الشمالية، إلى منضدة طعام مخصَّصة للبيض فقط في أحد متاجر أف. دبليو. وولورث بهدف الاعتراض على سياسة الشركة القائمة على التمييز العنصري. لم تُلغِ الاعتصامات التمييز على الفور، ولكنها أدت إلى حوار وطني انحلّ بموجبه التمييز العنصري في نهاية المطاف.

آمل في حال انضمام عدد كافٍ من الناس إليّ في رفض قبول الرَّقابة الكلّية الوجود غير المميِّزة أن نتمكن أيضاً من الحث على حوار تنحلّ بموجبه هذه الرَّقابة.

á á á

مع ذلك، لم أكن سعيدة بالأضرار التي ألحقتها تقنياتي المناهضة للرَّقابة بذهني. فكلما عرفتُ المزيد عمن يراقبني، ازداد ذُهاني الارتيابي أكثر فأكثر. وفي نهاية اختباري، وجدت نفسي رافضةً إجراء حوارات رقمية مع صديقاتي المقرَّبات بدون تشفير. وشرعتُ باستخدام اسمي الزائف للعمليات التجارية الزهيدة بشكل متزايد؛ صُدمت إحدى صديقاتي عندما حضرنا صف يوغا معاً وتسجّلتُ عرَضاً تحت اسم آيدا تاربيل.

لم أشأ العيش في العالم الذي أبني؛ عالم أحابيل ومعلومات زائفة وأعمال سرّية. إنه عالم قائم على الخوف. إنه عالم خالٍ من الثقة. ليس عالماً أريد تركه لابني وابنتي.

أذكر تعبير والدَيّ عن الشعور نفسه حيال التهديدَين الكبيرَين لجيلهما - الضرر البيئيّ وانتشار الأسلحة النووية. لم يشاءا أن يتركا لابنهما وابنتهما عالماً مدمَّراً بذَينك التهديدَين. بالطبع، لم نحلّ تماماً أيّاً من هاتَين المشكلتَين،

ولكننا احتوينا تهديد الأسلحة النووية من خلال معاهدات دولية، وخفّفنا من تأثير التلوث من خلال قوانين وضغط اجتماعي.

فالعِبَر المتخَذة من التنظيف البيئي مرتبطة بصفة خاصة بمشكلة الخصوصية. بالطبع، هناك المزيد مما يتعيّن القيام به، ولكن يجدر التذكير بمدى تلوّث الولايات المتحدة منذ مدة غير بعيدة. ففي العام 1969، اشتعلت بقعة زيت بنّيّة بلون الشوكولا في نهر كوياهوغا في كليفلند، أوهايو. لم تكن المرة الأولى التي تشتعل فيها أنقاض على النهر الشديد التلوّث قرب طواحين المدينة الفولاذية، ولم يكن الحريق الأسوأ على النهر. ولكن تغطية تايم ماغازين لحريق العام 1969 (المُرفَق بصورة مأساوية ومضلِّلة لحريق العام 1952 الأكثر تدميراً) كانت دعوة لاستيقاظ الأمّة. لقد قضينا العقود التالية في إعادة التفكير ملياً في عدم الإنصاف بالطلب من عامة الناس بتنظيف مخلَّفات الملوِّثين الصناعيين.

بكل المقاييس تقريباً، حققت إعادة التوازن إلى تحديد المسؤوليات في شأن التلوّث نجاحاً. فالهواء أكثر نظافة، والمياه أكثر نظافة، وأُنقذت الأنواع المهدَّدة. لم يكن في نهر كوياهوغا أسماك في أواخر الستينات، ولكن هناك الآن أكثر من أربعين نوعاً من الأسماك في النهر، لا بل أيضاً عدد قليل من بلح البحر الذي يعيش في المياه العَذبة، وهي دلالة على تحسّن نوعية المياه. (بالطبع، لقد تغاضينا عن مشكلة بيئية كبيرة - تراكُم ثاني أكسيد الكربون وغازات أخرى مسبِّبة للاحتباس الحراري وما نجم عنها من ارتفاع حرارة الأرض - نأمل في التطرّق إليها قريباً).

والخصوصية والتلوّث مشكلتان مماثلتان. فكلاهما يسببان ضرراً غير مرئي ومنتشر، وكلاهما ناجمان عن استغلال مورد ما - سواء أكانت أرضاً، مياهاً، أو معلومات. وكلاهما يعانيان من خاصيّات يصعب التعامل معها. ليس من السهل تحديد هويّة مادة ملوِّثة أو جزء واحد من البيانات يسبّب الضرر. ولكن غالباً ما يحدث الضرر بسبب تراكم مواد ملوِّثة، أو تجميع بيانات. والضرر الناجم عن التلوّث والخصوصية مشترك. فأحد لا يتحمل عبء التلوّث؛ كل المجتمع يعاني عندما يكون الهواء قذراً والمياه غير صالحة للشرب. بشكل مماثل، كلنا يعاني عندما نعيش في خوفِ استخدام بياناتنا ضدنا من قِبَل شركاتٍ تحاول استغلالنا أو ضباطِ شرطة يجرفوننا إلى صف لتمييز الوجوه.

لفهم الصلات بين الخصوصية والتلوث، اتصلتُ بدنيس هيرش، وهو أستاذ في القانون البيئي في كلّية حقوق جامعة العاصمة في أوهايو، درس

الخصوصية والقانون البيئي طوال عقد من الزمن. قارن هيرش مؤسسات تنقّب عن بيانات شخصية خاصة بأفراد لصالح مربِّي حيوانات يرعون ماشيتهم بشكل مُفرط في أراضٍ مُعشَوشبة مُشاعة، كما وُصفت في المقالة اللاحقة لغاريت هاردين العائدة للعام 1968 والتي نُشرت في مجلة ساينس ، "مأساة الأراضي المُشاعة". وصف هاردين كيف يسعى كل مربٍّ للحيوانات إلى زيادة أرباحه من خلال إضافة ماشية إلى قطيعه، عِلماً أن عدداً كبيراً من المواشي سيَرعون بشكل مُفرط ويُتلفون المرعى للجميع. كتب هاردين: "الحرية في الأراضي المُشاعة تحمل الدمار للجميع".

وصف هيرش التنقيب المُفرط عن البيانات بأنه مأساة مماثلة للأراضي المُشاعة. فعلى غرار راعي الماشية، قال، تملك الشركات التي تنقّب عن البيانات دافعاً لاستخدام مزيد من البيانات لتحقيق أفضلية تنافسية. ولكن كلما قاموا بذلك، قوّضوا ثقة المستخدمين بالعناية ببياناتهم بشكل ملائم وحمايتها. في نهاية المطاف، قال، يكفّ الأفراد عن الثقة بالشركات لحماية بياناتهم، ويكفّون عن الكشف عنها. وقال لي: "تكمن المخاطرة هنا في الإساءة كثيراً إلى ثقتنا في نهاية المطاف لدرجة انسحابنا من الويب".

إنه وصف جيد بالتأكيد لسلوكي الخاص. ففي تحقيقي عن شبكات التعقُّب، فقدت ثقتي بالمؤسسات التي تخزّن بياناتي. لقد سعيتُ للنجاة ببياناتي، ساحبةً إيّاها من الويب ومخزّنةً إيّاها في المنـزل. وأصبحتُ أيضاً متخصصة في المعلومات الزائفة، متخطيةً خوفي من الكذب في نشر أكاذيب عن عاداتي ونفسي.

من خلال النضال لحماية بياناتي، لوّثتُ الميدان العام وزرعت الشك. لا بد من وجود طريقة أفضل لمواجهة شبكات التعقُّب الجائرة.

á á á

تتمثل إحدى الطرق لتمهيد حقل الألعاب بممارسة الكل الرَّقابة.

إنه الجدل المطروح من قِبَل بعض التكنولوجيين، بمن فيهم ديفيد برين، المؤلّف الذي وصف في كتابه المجتمع الشفاف النشوءَ الحتميّ لرَقابةٍ (Surveillance) كلّية الوجود. يجادل برين، قائلاً إن الأمر الوحيد الذي سيُضعف نشوء دولة الرَّقابة هو نشوء ما يدعوه "رَقابة من تحت" (Sousveillance) حيث يراقب المواطنون الحكومة من تحت بعدائية مماثلة لعدائية مراقبة الحكومة لهم.

بالتأكيد، إن واقع قيام كل مواطن الآن بحمل كاميرا مدمَجة بهاتف محمول جعل الشرطة مسؤولة أكثر فأكثر عن أعمالها. على سبيل المثال،

طُرد ضابط شرطة رشّ طلاّباً معترضين لا عنفيين برذاذ الفُلفل، في جامعة كاليفورنيا في ديفيس عام 2011، بعد نشر فيديو لما قام به على الملأ.

أصبحت الرَّقابة من تحت نشاطاً مناهضاً للحرب أيضاً. ففي العام 2010، أطلق الممثل جورج كلوني والناشط في ميدان حقوق الإنسان، جون برندرغاست، برنامج رَقابة عبر قمر صناعي لمراقبة الحرب الأهلية في السودان. وفي أيار/مايو 2013، قدّم مشروع سنتينيل عبر الأقمار الصناعية، التابع لكلوني وبرندرغاست، دليلاً على تلكّؤ السودان وجنوب السودان في الإيفاء بالتزاماتهما لسحب جنود من المنطقة المنـزوعة السلاح على امتداد الحدود.

ولكن، لسوء الحظ، هناك كثير من الأعمال الحكومية التي لا يمكن للمواطنين التحكم بها بواسطة كاميرات أو أقمار صناعية. فما كنا لِنَعرف أبداً عن شبكات تعقُّب وكالة الأمن القومي للمواطنين الأميركيين الأبرياء لو لم يكشف إدوارد سنودن أمرها. وما كنا لِنعرف على الأرجح مقدار ما يُنفَق من أموال دافعي الضرائب لتمويل شبكات التعقُّب تلك بدون إفشاءات سنودون عن "الميزانية السوداء" التابعة لوكالات الاستخبارات.

ما كنا لِنرى ربما الفيديو المثير للقشعريرة ومشاهد قيام جنود أميركيين بإطلاق النار على صحافيين وأطفال أبرياء من طائرتهم في بغداد لو لم يكشف أمره الجندي برادلي مانينغ. وما كنا لِنحصل على الأرجح على رواية دقيقة عن مقتل المدنيين في حربَي العراق وأفغانستان لو لم يكشف مانينغ عن مئات آلاف السجلات عن الحرب.

ولكن إفشاءات سنودن ومانينغ غير مميِّزة أيضاً. لقد حصل كلاهما على مجموعات قيّمة من المستندات رسمت، بالإجمال، صورة أكثر شمولية من أي مستند آخر. كانا يُخضعان الحكومة، إلى حد ما، لرَقابة من تحت مستخدمَين شبكات تعقُّب معلومات خاصة بهما.

ولكن ثَبُت أن الحكومة لا تحب الوقوع في فخ شبكات التعقُّب أكثر مما أوقعتُها في فخ أحابيلي. لقد وجّهت إدارة أوباما كل التُّهَم الممكن توجيهها إلى مانينغ وسنودن، متهمةً إيّاهما بمجموعة من الجرائم، من بينها التجسس. وفي العام 2013، حُكم على مانينغ بالسجن لمدة خمسة وثلاثين عاماً، وحصل سنودن على لجوء سياسي مؤقّت في روسيا.

ولكن لم تتم مقاضاة سنودن ومانينغ فقط بسبب جهودهما لكشف النقاب عن سلوك الحكومة، بل يُستهدَف أيضاً، وبشكل متزايد، صحافيون تقليديون من خلال تحقيقات جنائية - يلازمون الخطوط الأمامية لمراقبة

الحكومة. ففي العام 2013، أبلغت وزارة العدل الأسوشيتد بريس - بعد الحادثة - بأنها حصلت على سجلات اتصالات هاتفية لعدة صحافيين في وكالة الأنباء جرت لمدة شهرَين، كجزء من تحقيق حول تسريب معلومات عن عملية الـسي آي أيه في اليمن. لقد اعترض غاري برويت، رئيس الـأيه بيي والمدير التنفيذي، على التطفل، قائلاً، "نعتبر عمل وزارة العدل هذا تدخلاً سافراً بحقوق الـأيه بيي الدستورية في جمع ونقل الأخبار".

وتضغط وزارة العدل على مراسل نيويورك تايمز ، جيمس رايزن، كي يكشف عن مصادره التي استعان بها لوضع كتاب يكشف عن عملية الـسي آي أيه غير المُتقَنة، متهمين إيّاه بتزويد علماء إيرانيين بمخططات تفصيلية مليئة بالأخطاء لجهاز نووي. كان رايزن قد أعلن إنه سيذهب إلى السجن بدلاً من تقديم شهادة عن مصادره.

من غير المحتمَل أن تمهّد الرَّقابةُ المتبادَلة حقلَ الألعاب إذا استخدمت الحكومة نفوذها لمقاضاة أولئك الساعين إلى تحميل الحكومة مسؤولية أعمالها.

á á á

هناك طريقة ممكنة أخرى لتحميل مشغّلي شبكات التعقُّب مزيداً من المسؤولية عن أعمالهم: توجيه التُّهَم إليهم، ببساطة، بولوج بياناتنا الشخصية.

هذه الفكرة مُغوِية ببساطتها. سأطالب باستعادة بياناتي الشخصية، وأضعها في خزنة وهمية، وأبيع بعضها في السوق المفتوحة - بدلاً من "أخذها" مني. لقد نشأ عدد قليل من الشركات في المرحلة الأولى من عملياتها على أمل خصخصة سوق البيانات الشخصية. وفي العام 2011، أعلن منتدى الاقتصاد العالمي أن البيانات الشخصية تظهر للعيان كـ"نوع جديد من الأصول".

ولكن حتى الآن، تبقى البيانات الشخصية أصولاً قيد الإنجاز، ويعود سبب ذلك إلى سهولة طلبها وتوفيرها: لا أملك النسخة الوحيدة عن بياناتي بما أنه لا وجود لقانون يُلزم وسطاء البيانات بإعادتها لي. لذلك، لن يقوم أحد بدفع مبلغ كبير لي لاستخدام نسخة بياناتي، في حين يمكنه الحصول عليها من مكان ما بسعر أقل.

لقد وجد تحليل لفايننشال تايمز أن كلّية وجود البيانات الشخصية خفّضت الأسعار لدرجة أن معلومات تتناول عمر شخص عادي، وجنسه، ومكان إقامته، تكلّف جزءاً من السِّنت. ويُباع المجموع الكلّي للمعلومات عن معظم الناس بأقل من دولار واحد. لقد أدخلتُ معلوماتي إلى الآلة

الحاسبة للبيانات في فايننشال تايمز ووجدتُ أن معلوماتي تساوي 28 سنتاً.

قد تساعد القوانين التي تمنح الناس مِلكية بياناتهم - كلّياً أو جزئياً - على رفع سعر البيانات. ولكن الأمر سيتعقّد بسرعة كبيرة. فبالرغم من كل شيء، كيف أشاطر مِلكية بيانات اتصالاتي الهاتفية مع أيه تي أند تي؟ وكيف أحول دون قيام الحكومة بالحصول على بياناتي المملوكة جزئياً من أيه تي أند تي؟

ولست واثقة من أن بيع البيانات سيؤدي إلى الحد من تأثيرات الرَّقابة المثيرة للقشعريرة. من قبل، كان لدينا أَجر بالحد الأدنى وساعات عمل محدودة، وكان الناس مستعدّين لبيع عملهم بأسعار منخفضة للغاية لقاء ساعات عمل طويلة.

وجد أليساندرو أكويستي، وهو أستاذ في جامعة كارنجي ميلون يُجري دراسات على الجوانب الاقتصادية للخصوصية، أن الناس أقل استعداداً للدفع لقاء الخصوصية التي لا يملكونها. ففي أحد الاختبارات، قدّم أكويستي وزملاؤه الباحثون لمجموعة من الأشخاص بطاقة فيزا مجانية بقيمة 10 دولارات، وطلبوا منهم أن يكون إنفاقهم غُفلاً. وقدّموا لمجموعة أخرى بطاقة فيزا مجانية أخرى بقيمة 12 دولار، وطلبوا منهم أن يكون إنفاقهم علنياً. بعد ذلك، قدّموا لأفراد من كل مجموعة فرصة مقايضة بطاقاتهم ببطاقات المجموعة الأخرى. لقد احتفظ اثنان وخمسون من حاملي بطاقات الدولارات العشرة ببطاقاتهم - موافقين، في الواقع، على دفع دولارَين للمحافظة على خصوصيتهم. ولكن ما يزيد عن 90 بالمئة من حاملي بطاقات الدولارات الاثنَي عشر رفضوا المقايضة - مما يعني أنهم رفضوا التخلي عن الدولارَين لحماية خصوصيتهم. وقد قال لي أكوسيتي: "يعني ذلك أن الناس يقدّرون بعض الأشياء عندما يملكونها أكثر من تقديرهم لها عندما لا يملكونها".

في الأساس، عندما لا تتمتعون بالخصوصية، تشعرون بألم أقل إذا فقدتموها. بدلاً من ذلك، تشعرون بألم اضطراركم لـ"إعادة شراء" الخصوصية. فهذا العجز عن تحديد قيمة بياناتنا بدقة هو أحد أسباب إخفاق معظم المنتجات المُباعة لحماية الخصوصية، وجعل الرَّقابة الكلّية الوجود ممكنة وشرعية بعد تحويل البيانات الشخصية إلى عُملة - بدون أية تشريعات تمكّن من جعل البيانات الشخصية نادرة، وبالتالي أكثر قيمة.

á á á

وهكذا، أعود بتردد إلى القوانين للحد من رَقابة شبكات التعقُّب.

ويعود سبب ترددي إلى أن قوانين الخصوصية تملك سجل إنجازات هزيل في الولايات المتحدة. فبخلاف معظم الدول الأوروبية، لا يوجد في الولايات المتحدة قانون خصوصية شامل يُلزم جامعي البيانات بتلبية بعض المعايير بالحد الأدنى، بل هناك قوانين خصوصية تغطي بعض القطاعات - الصحة، المال، الأطفال، والسجلات الحكومية. ومعظم هذه القوانين القطاعية تُلزم جامعي البيانات بالكشف عن كيفية تصرّفهم بالبيانات وبالسعي إلى موافقة المستخدمين على استخدام معلوماتهم الشخصية. تبدو فكرة جيدة، ولكن ثَبُتت عملياً سهولة التحايل على الإشعار والموافقة.

إن قانون حماية خصوصية الأطفال عبر الإنترنت هو خير مثال على ذلك. فبدلاً من الحصول على موافقةٍ والديّة لجمع عناوين البريد الإلكتروني للأطفال، تُؤثِر الشركات أن تبقى جاهلة لوجود أطفال على مواقع الويب الخاصة بها.

أو تأمّلوا بقانون إخضاع التأمين الصحي لقابلية النقل والمحاسبة العائد للعام 1996 الذي يُفترض به تمكين الناس من ولوج سجلاتهم الطبية، مما يسمح لهم بتسليم مزوِّدهم التالي بالسجلات. هو ينهى أيضاً عن بيع البيانات الصحية التي يمكن تحديد هوية أصحابها لغايات تسويقية، ولكن البيانات "الغُفل" مُعفاة من القيود إلى حد كبير. نتيجةً لذلك، تمارس عدة صيدليات تجارة مُربِحة من خلال بيع سجلات وصفات طبّية غُفل لقواعد بيانات وطنية عملاقة. (حاولت فيرمونت حظر بيع السجلات الصيدلانية، ولكن المحكمة العليا أوقفت العمل بقانونها، مشيرةً إلى أن القيود التي يفرضها على النشاطات التسويقية لمصنّعي المنتجات الصيدلانية تنتهك التعديل الأول).

أو تأملوا بقانون الخصوصية الفيدرالية الذي يُفترض به إرغام الوكالات الفيدرالية على الحصول على الموافقة قبل تشاطر معلومات عن المواطنين مع وكالات أخرى لغايات غير "منسجمة" مع سبب جمع البيانات في الأصل. ولكن بدلاً من طلب الموافقة، تصف الوكالات ببساطة تشاطر البيانات في ما بينها بأنه "استخدام روتيني" لا يطاله القانون. نتيجةً لذلك، أخفق قانون الخصوصية في الحؤول دون تحميل المركز القومي الأميركي لمكافحة الإرهاب كلَّ قواعد البيانات التي تحتوي على ملفات المواطنين من وكالات حكومية أخرى بهدف البحث عن إلماعات إرهابية.

يبدو أن الأمر انتهى بقوانين الخصوصية، المستندة على الموافقة، إلى ابتكار موافَقة مصطنَعة.

á á á

ولكن قوانين الخصوصية التي تمنح الناس حق رؤية البيانات المستخدَمة ضدهم تبدو فكرة جيدة.

تأملوا بظُلم قائمة مراقبة الإرهاب. ففي العام 2009، ذهب محمد القرّه غولي، وهو مواطن أميركي وُلد في الصومال وهاجر إلى الولايات المتحدة عندما كان في الثالثة من عمره، لزيارة أنسبائه في الصومال لمدة أشهر عدة، ومن ثم انتقل إلى الكويت للدراسة والإقامة مع أحد أعمامه.

في 20 كانون الأول/ديسمبر 2010، ذهب محمد إلى مطار الكويت لتجديد تأشيرة دخوله، كما كان يفعل كل ثلاثة أشهر منذ وصوله. أثناء وجوده في المطار، دنا منه رجلان، وكبّلا يدَيه، وعصبا عينَيه، واقتاداه إلى مكان لم يُكشف عنه. يقول محمد، الذي كان في الثامنة عشرة من عمره فقط في ذلك الوقت، إنه تعرّض للتعذيب طوال أكثر من أسبوع، وضُرِبَ بالعصي، وأُرغم على الوقوف لفترات طويلة؛ في إحدى المرات، بقيت ذراعاه موثَّقتَين بعارضة في السقف حتى أُغمي عليه. لقد استُجوب في شأن الزعيم المتشدد أنور العولقي.

في 28 كانون الأول/ديسمبر، نُقل إلى منشأة للترحيل حيث زاره عملاء أف بـي آي. فرفض الإجابة عن أسئلتهم دون وجود محامٍ، وقالوا إنه سيُعتقَل مدة غير محدَّدة إذا لم يُجب عن الأسئلة. في 12 كانون الثاني/يناير، زاره عملاء أف بـي آي ثانيةً، ورفض مجدداً الإجابة عن أسئلتهم. أخيراً، في 6 كانون الثاني/يناير من العام 2011، اصطحبه مسؤول كويتي إلى المطار وأعطاه تذكرة طيران إلى الولايات المتحدة اشترتها له عائلته. مع ذلك، لم يُسمح لمحمد بدخول الطائرة لأنه كان على قائمة حظر الطيران. في نهاية المطاف، سُمح له بالسفر جوّاً إلى وطنه في 21 كانون الثاني/يناير. ولكن لم يَعُد بإمكانه السفر جواً مذاك الحين.

لقد أُثيرت محنة محمد على الأرجح بسبب بيانات شخصية جُمعت عنه. ولكن لم يُسمَح له برؤية تلك البيانات، بل جادلتِ الحكومة، قائلةً إنه يُفترض به طلب تعويض من خلال تقديم شكوى ضد برنامج الاستعلام عن التعويض على المسافرين التابع لوزارة الأمن الداخلي. يمكن للمسافرين الذين يُمنعون من الصعود إلى متن الطائرات تقديم معلوماتهم للوزارة التي تخمّن ما إذا كانوا قد استُهدفوا بشكل غير صحيح لأنهم يتشاطرون الاسم مع شخص ما على قائمة المراقبة، أم بسبب سوء تفاهم آخر. مع ذلك، لا يُطلب من الوزارة منح الأفراد الموجودين على قائمة المراقبة فرصة للاعتراض

رسمياً على إدراجهم فيها؛ في الواقع، لا تؤكد الوزارة أو تنفي أبداً ما إذا كانوا على القائمة. يدّعي محمد بأنه يُحرم من حقه الدستوري باللجوء إلى الإجراءات القانونية المناسبة عندما يُمنَع من "آلية قانونية وافية دستورياً" للاعتراض على إدراجه في قائمة حظر الطيران.

إنه النوع الأسوأ لإساءة استعمال البيانات الشخصية: لقد تعرّض محمد للتعذيب ولا يمكنه الصعود إلى متن طائرة حتى يومنا هذا لأسباب لا يعرفها، وقيل له إنه لا يمكنه الاعتراض على تلك الأسباب في محكمة العدالة. ليست كل إساءات استعمالِ البيانات بغيضة بالمستوى الذي بلغتْه في حالة محمد، ولكن محنته تذكّرني بمدى أهمية وجود آلية للسماح للناس برؤية البيانات المستخدمة ضدهم.

هناك حركة متنامية لتحميل الشركات مسؤولية البيانات التي يملكونها عن الأفراد. فالاتحاد الأوروبي يُلزم الشركات بأن توفر للمواطنين إمكانية ولوج البيانات المتعلقة بهم. ففي العام 2011، اقترح السيناتوران جون ماكين وجون كيري تشريعاً للخصوصية التجارية يُلزم جامعي البيانات بأن يوفروا للأفراد إمكانية ولوج بياناتهم، وفرصة لاختيار عدم الاشتراك ورفض مشاطرة بياناتهم مع أطراف ثالثة. ولكن مؤيّدين للخصوصية ووسطاء بيانات قاوموا التشريع الذي لم يحقق أي تقدم. في العام 2012، أعلنت إدارة أوباما أنها لن تنتظر اتخاذ الكونغرس قراراً في شأن الخصوصية، وأطلقت مسعى لحمل صناعة البيانات التجارية على تطوير إذعانٍ طوعيّ لمعايير الخصوصية، بما فيها توفير إمكانية ولوج الأفراد بياناتهم.

تتمثل إحدى الطرق الأكثر نجاحاً لجعل وسطاء البيانات مسؤولين أمام القانون بقانون التقرير الائتماني العادل الذي يسمح للناس بولوج، وتصحيح، ومناقشة البيانات التجارية المستخدَمة لتقييمهم بهدف اتخاذ قرارات مالية. نتيجةً لذلك، وبالرغم من احتواء تقريري الائتماني على معلومات غير دقيقة، كان من السهل عليّ تصحيحها. ويُلزم القانون أيضاً كل من يستخدم تقريري الائتماني لحرماني من قَرض، تأمين، أو وظيفة، بإطلاعي على السبب الكامن وراء الرفض ومنحي فرصة لمناقشة المعلومات.

بالطبع، لقانون التقرير الائتماني عيوبه. قد يكون من الصعب جداً مناقشة البيانات الموجودة في التقارير الائتمانية؛ هو يغطي أنواعاً معيّنة من القرارات المالية. ويسهل على وسطاء البيانات الكبار أن تكون لديهم ملفات مفصَّلة عن الأفراد كي يدّعوا أن بياناتهم لا يشملها القانون. فشركة تحديد مخاطر الائتمان، إي بيرو، التي وضعتني في خانة أولئك الذين لم يُتِمّوا

دراستهم الثانوية، مثلاً، تقول إن تحليلاتها تُستخدَم لـ"تقييم" الأشخاص لغايات تسويقية، وليس للتصديق على إمكانية حصول الناس على حساب ائتمان، قَرض، أو تأمين - مما يعني أن تحليلاتها لا يغطيها القانون.

لقد أوصت مندوبة لجنة التجارة الفيدرالية، جولي بريل، بتوسيع القانون ليشمل نطاقاً أوسع من استخدام البيانات، ولا سيما إذا كانت البيانات الشخصية مستخدَمة لاتخاذ قرار في شأن "ما إذا كنا نخاطر جداً باستخدامها لأعمال تجارية أم أنها غير مناسبة لبعض النوادي، خدمات المواعدة، مدارس، أو برامج أخرى". وطلبت من وسطاء البيانات منح الأفراد، طوعاً، حق ولوج بياناتهم، والفرصة لتصحيح بياناتهم، واختيار عدم الاشتراك إذا كانت البيانات مستخدَمة لغايات تسويقية. ولكن بما أن لجنة التجارة الفيدرالية غير مخوَّلة وضع قوانين بسهولة - بخلاف وكالة الحماية البيئية - فكل ما يمكن لبريل القيام به هو تشجيع صناعة البيانات على تنظيم ذاتها، ما لم تتخطَ نشاطات الصناعة حدودها وتنتهك قوانين أكثر عمومية فيطالها، كما في السابق، منعُ الممارسات "الجائرة والمضلِّلة" الصادر عن لجنة التجارة الفيدرالية.

في اقتصادٍ قائم على المعلومات، قد نكون بحاجة إلى وكالة لحماية المعلومات تملك صلاحية تنظيم هذا الاقتصاد، مع تركيز خاص على شفافية معالجة البيانات واستخدامها والمسؤولية المترتبة على ذلك.

á á á

ولكن إنشاء وكالة لحماية المعلومات فقط لن يكون كافياً لإجراء رَقابة حكومية أو لمعالجة محنة أشخاص مثل محمد القرّه غولي.

في ما يتعلق بالرَّقابة الحكومية، لقد ملنا إلى التسليم بشبكات التعقُّب عندما تفوق الفوائدُ التي تعود على المجتمع تأثيراتِ انتهاك الخصوصية الناجمة عن التطفّل على المعلومات الشخصية. نحن نتساهل مع زيارات مفاجئة يقوم بها مفتشون حكوميون إلى أماكن العمل، ونسمح للشرطة بإقامة حواجز تعقُّب في الطرقات بهدف البحث عن سائقين مخمورين، ونتحمّل اختبار مستوى المخدرات في الجسم في بعض أماكن العمل.

ولكننا لا نقبل شبكات تعقُّب متطفّلة جداً لتحقيق غاياتها. لقد رفضنا ماسحات الأجساد في المطارات التي تكشف عن الخطوط الكفافية لأجساد الأفراد العارية. نحن لا ندسّ رقاقات تعقُّبية بالغة الصِّغَر تحت بشرة أطفالنا كما نفعل مع الكلاب الأليفة، ولا نثبّت كاميرات رَقابة في

الحمامات.

نطالب بألا تكون شبكات التعقُّب الحكومية تمييزية من منطلَق عِرقي. ففي العام 2013، حكمت القاضية شيرا شيندلين في المحكمة الجزئية الفيدرالية على أن شبكة تعقُّب قسم شرطة نيويورك "ستوب إند فريسك" (stop and frisk) تنتهك الدستور من خلال استهداف شبان سود ورجال إسبان لا شُبهة عليهم. وقد دونت: "لا يُفترض بأحد أن يعيش في ظل خوفِ إيقافه كلما غادر منـزله لممارسة نشاطاتِ حياته اليومية".

بالطبع، لقد سمحنا أحياناً في حُمّى زمن الحرب، لشبكات التعقُّب الحكومية بالذهاب بعيداً في قراراتها. ففي العام 1944، حكمت المحكمة العليا بأن اعتقال أكثر من مئة ألف أميركي من أصل ياباني أثناء الحرب العالمية الثانية هو أمر قانوني لأنه "يستحيل التمييز بشكل فوري بين الموالين وغير الموالين". وفي خلاف مَشوب بالعاطفة، كتب القاضي فرانك مورفي، "يتخطى الحكم شفير السلطة الدستورية ويقع في هوّة العِرقية القبيحة".

مع ذلك، وبالرغم من زلاّتها، وضعت المحكمة، كما يبدو، في السنوات الأخيرة مجموعة مُقنعة من الأسئلة لمعرفة متى تكون شبكة التعقُّب منصفة:

- هل شبكة التعقُّب تطفّلية جداً لتحقيق غايتها؟
- هل تفيد المجتمع؟
- هل تقع في هوّة العِرقية القبيحة (أو في تحيّزات أخرى)؟

لقد ذكّرتني هذه المعايير غير واضحة المعالم باختبار الإعلان جَهاراً الذي اعتمدتُ لتقييم ما إذا كان باستطاعتي تبرير كذبـي في شأن هويّتي. في ذلك الوضع، قررت أن الشخص المنطقي سيؤيّد أكاذيبـي لأنها محدودة ولا يراد بها إلحاق الأذى، ولأنها محاولتي لمعالجة وضع غير مُنصِف. الآن، غداة إفشاءات إدوارد سنودن، يقيّم الجمهور ما إذا كانت شبكات تعقُّب وكالة الأمن القومي نجحت في اختبار الإعلان جَهاراً.

يذكّر هذا الاختبار أيضاً بأحد التكتيكات الأكثر فعالية للحركة البيئية. كل عام، تنشر وكالة الحماية البيئية في الجردَة السنوية للانبعاثات السامة قائمةً بالشركات التي تخزّن المواد الملوِّثة الأكثر سُمّية. لقد أدى نشر القائمة إلى تنافس الشركات على تخفيض انبعاثاتها السامّة إلى الحد الأدنى. "الكل يريد تجنّب التواجد في المراتب الأولى لتلك القائمة"، قالت ليزا هينـزرلينغ، وهي أستاذة في القانون البيئي في جامعة جورج تاون. "كان نجاحاً باهراً".

لقد تساءلتُ عما إذا كان الحل لشبكات التعقُّب الحكومية دفعة مماثلة في اتجاه الشفافية. هذا هو جوهر النقاش الذي أثاره كريستوفر سلوبوغين، وهو أستاذ قانون في جامعة فاندربيلت أجرى دراسات موسَّعة عن شبكات التعقُّب الحكومية. هو يقترح وجوب قيام المحاكم بحظر شبكات التعقُّب الحكومية التي لا تُجيزها التشريعات بصفة خاصة. "في حين نترك المحاكم منهمكة بقانون البحث والضبط في قضايا فردية، تتعزز القِيَم الديموقراطية... عندما يطال البحث والضبط مجموعات"، كتب. علاوةً على ذلك، يقترح منح المحاكم القدرة على كبح جماح شبكات التعقُّب إذا كانت شديدة التطفّل أو منحازة ضد مجموعة معيَّنة.

باختصار، هو يجادل، قائلاً إنه يجب على شبكات التعقُّب الحكومية ألا تكون سرّية. يجب التدقيق بها إما من قِبَل هيئة تشريعية أو محكمة.

á á á

إن شبكات التعقُّب الخاصة بالرَّقابة جائرة بطبيعتها، فتمسك بالبريء والمُذنب بطريقة غير مميِّزة، موجِدةً بهذه الطريقة ثقافة خوف - حيث يخشى أشخاص مثل شارون جيل وبلال أحمد من التحدث عبر الإنترنت عن مشاكلهم العقلية، وحيث يقطع ياسر عفيفي صداقته بصديقه الذي يقول أموراً خرقاء عبر الإنترنت.

حسناً، إن الحياة جائرة. ويصبح السؤال: ما مِقدار الجَور المقبول؟

نحن نُطيق الكثير من الجَور في المجتمع. فبعض الأشخاص أثرياء وبعضهم الآخر فقير. بعض الصغار يرتادون مدارس عامة جيدة وبعضهم الآخر يرتاد مدارس عامة مريعة. بعض الناس يعيشون قرب حدائق عامة ونباتات خضراء جميلة بينما يعيش آخرون في أماكن لا مساحة خضراء فيها.

ولكن هناك جَور لا نُطيقه. نحن لا نُطيق الناس يسرقون ويُفلتون من العقوبة. لا نُطيق الرشوة. لا نُطيق شركات تبيع سلعاً تُلحق الأذى بالناس.

يتبدّل حسّنا بالإنصاف على مَرّ الزمن. لقد اعتدنا التفكير من أنه من المُنصف للصغار أن يعملوا ساعات طويلة على خطوط التجميع. بعد ذلك، كففنا عن التفكير في ذلك. اعتدنا التفكير في أنه من المُنصف للشركات أن تلوّث أنهارنا وسماواتنا. بعد ذلك، كففنا عن التفكير في ذلك. واعتدنا التفكير في أنه من المُنصف ترك معلومات مرتبطة بكلبنا على الرصيف، وكففنا بعد ذلك عن الأمر.

كمواطنين في بلد ديموقراطي، علينا القيام بهذه القرارات.

بالنسبة إلى شبكات تعقُّب البيانات، وجدنا أن الشفافية وإمكانية التعرض للمحاسبة تنسجمان مع التقارير الائتمانية. وشهدنا المعايير التي يعتمدها القضاة لتقييم شبكات التعقُّب. بجمع كل ذلك مع اختبار الإعلان جَهاراً، أعتقد أن باستطاعتنا وضع قائمة من ستة أسئلة يُفترض طرحها حول كل شبكة تعقُّب:

- هل توفر شبكة التعقُّب للأفراد الحق القانوني لولوج بيانات، وتصحيحها، ومناقشتها؟
- هل يحمَّل مشغّلو شبكة التعقُّب المسؤولية حول كيفية استخدام البيانات؟
- هل إن شبكة التعقُّب تطفّلية كثيراً لتحقيق غايتها؟
- هل تُفيد المجتمع؟
- هل تقع في هوّة العِرقية القبيحة (أو في تحيّزات أخرى)؟
- هل يمكنها تحمّل تدقيق علنيّ؟

بطرح هذه الأسئلة عن كل شبكة تعقُّب، آمل في أن نتمكن من التمييز بين شبكات التعقُّب غير المُنصفة على نحو لا يُطاق وتلك التي يمكننا تحمّلها.

فبعض شبكات التعقُّب التكنولوجية القائمة حالياً لن تنجح في الاختبار. تأملوا بالتعقُّب عبر الإنترنت والتعقُّب الذي يقوم به التجار بالمفرّق. فبتتبّع نقراتنا على المفاتيح عبر الإنترنت، أو بتتبّع هواتفنا المحمولة في مركز تسوّق، يكون المتتبّعون تطفليين كثيراً كي يحققوا هدفهم التسويقي المستهْتر، كما أنهم لا يوفرون أية فرصة لأجل التصحيح.

أو تأملوا بشبكات تعقُّب وكالة الأمن القومي. ما يزال على الوكالة تقديم دليل مُقنِع على أن شبكاتها المتعقِّبة لأميركيين أبرياء أفادت المجتمع بما يكفي لتخطّي تطفّلها. فالأفراد لا يمكنهم ولوج بياناتها، وتغطي محكمة سرّيّة قانونية شبكات التعقُّب الجارفة للمعلومات.

أو تأمّلوا بتسلل قسم شرطة نيويورك إلى مساجد مسلمة ومجموعة من المجتمع من خلال شبكة تعقُّبٍ عِرقيةِ الاستهداف تبدو كما لو أنها وقعت في هوّة العِرقية البغيضة.

ولكن قد تنجح شبكات تعقُّب أخرى في الاختبار. فاستخدام الشرطة لكاميرات الرَّقابة ولوحات التسجيل يمكن أن تكون مفيدة للمجتمع بما يكفي لتبرير تطفّلها، ولا سيما إذا مُنح مجرمون مزعومون فرصة الاعتراض

على التُّهَم الموجَّهة إليهم في المحكمة. وقد ينجح وسطاء البيانات الذين يحمَّلون مسؤولية بياناتهم - على غرار وكالات التصنيف الائتماني - في الاختبار أيضاً.

حتى إن المتبارين بأسلوب حر، مثل غوغل وفيسبوك، قد ينجحون في اختبار الإنصاف إذا حدّوا من تطفّل تعقُّبهم، ووفّروا إمكانية ولوج بياناتهم بشكل حقيقي يحمل معنى أكبر، وحُمّلوا مسؤولية البيانات التي يتشاطرونها مع آخرين.

من المؤكَّد تقريباً أن قائمة جَرْدي في شأن الجَور ليست دقيقة. ولكنها محاولة لشق طريق وسطيّ بين أولئك الذين يطلبون منا تسليم كل بياناتنا و"تناسي الأمر"، وأولئك الذين يقترحون علينا رَمي أنفسنا على سكة الحديد أمام قطار الاقتصاد المُسرع القائم على بياناتنا. لا أحد، بمن فيهم أنا، يريد التخلي عن كل فوائد الاقتصاد القائم على بياناتنا - بوجود خرائطه ووقائعه السحرية عند أطراف أصابعنا، والقدرة على الاتصال بأي شخص في العالم بلحظة. ولكن لا يُفترض بأيٍّ منا التخلي ببساطة عن كل بياناتنا بدون أية ضمانات لعدم ارتدادها علينا لتعضّنا.

لم نُغلق الاقتصاد الصناعي لإيقاف التلوّث، بل طلبنا من الملوِّثين ببساطة تحمّل مسؤولية أكبر عن أعمالهم. لقد أقرّينا قوانين، وابتكرنا وكالة حكومية جديدة، وأرغمنا الملوِّثين ليكونوا شفّافين. بشكل مماثل، لسنا بحاجة إلى إغلاق الاقتصاد القائم على البيانات. نحن بحاجة فقط إلى حمل مالكي البيانات على السماح لنا برؤية ما يملكونه عنا وبتحمل مسؤولية أي أذى يتسببون به جرّاء استخدام بياناتنا.

إذا نجحنا في العثور على طريق وسطيّ، قد نجد أنفسنا في عالم جديد برّاق حيث لا تكون الخصوصية مستهدَفة بذاتها. قد نجد أن الخصوصية كانت مجرد دِرع نحمله لحماية أنفسنا من الأذى. وإذا تمّ احتواء الأذى، قد نتمكن من إنـزال الدّرع بما يكفي ليتمكّن صغارنا من نشر فيديوهاتهم الخاصة على يوتيوب، وليتمكن بلال وشارون من تجديد حواراتهما على منتدى PatientsLikeMe الطبّي، وليتمكن ياسر وخالد من استعادة صداقتهما القائمة منذ الصِّغر.

سيكون عالَماً أريد لصغيرَيَّ أن يعيشا فيه.

انتهى

[1] الباباراتسو مصوِّر صحافي يلاحق المشاهير لتصويرهم على حين غَفلة.

[2] سوق في العراء لبيع أشياء وملابس مستعملة رخيصة.

[3] تدعى أيضاً "قصر الذاكرة".